

John T. Conway, Chairman  
A.J. Eggenberger, Vice Chairman  
John E. Mansfield  
R. Bruce Matthews

## DEFENSE NUCLEAR FACILITIES SAFETY BOARD

625 Indiana Avenue, NW, Suite 700, Washington, D.C. 20004-2901  
(202) 694-7000



December 14, 2004

The Honorable Spencer Abraham  
Secretary of Energy  
1000 Independence Avenue, SW  
Washington, DC 20585-1000

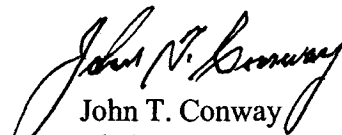
Dear Secretary Abraham:

The Defense Nuclear Facilities Safety Board (Board) issued Recommendation 2004-1, *Oversight of Complex, High-Hazard Nuclear Operations*, on May 21, 2004. On July 21, 2004, the Department of Energy (DOE) accepted Recommendation 2004-1. The enclosed technical report, DNFSB/TECH-35, *Safety Management of Complex, High-Hazard Organizations*, provides background information and ideas for implementing the Recommendation.

The report explores organizational aspects of safe operations with the intent of helping to identify how DOE could better organize itself to enhance safety, particularly nuclear safety. Academic research on organizations involved in operations with the potential for high-consequence accidents and lessons learned from major accidents and near-misses are summarized. The foundations for nuclear safety within DOE are then described, and a set of organizational attributes are proposed for safely managing operations that can lead to high-consequence, low-probability accidents. The report then describes DOE's proposed safety management changes and explains why the Board regards those changes as cause for concern. The proposed organizational attributes are applied to evaluate DOE's safety management of its high-hazard operations. Finally, suggested improvements to DOE's safety management of these operations are presented.

The ideas presented in the report are not intended to represent the only way to satisfy the Board's recommendation, but to provoke innovations and new solutions for a sustained organizational shift that should better ensure the safe management of high-hazard nuclear operations.

Sincerely,

  
John T. Conway  
Chairman

c: The Honorable Linton Brooks  
Mr. Mark B. Whitaker, Jr.

Enclosure

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>DEC 2004</b>		2. REPORT TYPE		3. DATES COVERED -	
4. TITLE AND SUBTITLE <b>Safety Management of Complex, High-hazard Organizations</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Defense Nuclear Facilities Safety Board, 625 Indiana Avenue SW Suite 700, Washington, DC, 20004</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT <b>see report</b>					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES <b>57</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

# **SAFETY MANAGEMENT OF COMPLEX, HIGH-HAZARD ORGANIZATIONS**

---

**Defense Nuclear Facilities Safety Board**

**Technical Report**



**December 2004**

# **SAFETY MANAGEMENT OF COMPLEX, HIGH-HAZARD ORGANIZATIONS**



This report was prepared for the Defense Nuclear Facilities Safety Board by Board Member R. Bruce Matthews with assistance of former Deputy Technical Director James J. McConnell and former Board Member Joseph J. DiNunno.

## EXECUTIVE SUMMARY

The Department of Energy (DOE) is implementing or contemplating a variety of changes in the management and contract processes that define, govern, and oversee the operations of DOE contractors performing defense nuclear activities. These well-intended changes, designed to improve productivity and efficiency, have the potential to lessen safety and to make a high-consequence, low-probability accident more likely. This report summarizes academic research on organizations involved in high-consequence operations, as well as lessons learned from major accidents and near-misses. Organizational attributes are identified that should benefit the safe management of nuclear operations. Corrective actions have been recommended to DOE as part of the Defense Nuclear Facilities Safety Board's (Board) Recommendation 2004-1, *Oversight of Complex, High-Hazard Nuclear Operations*.

Many of DOE's national security and environmental management programs are complex, tightly coupled systems with high-consequence safety hazards. Mishandling of actinide materials and radiotoxic wastes can result in catastrophic events such as uncontrolled criticality, nuclear materials dispersal, and even an inadvertent nuclear detonation. Simply stated, high-consequence nuclear accidents are not acceptable. Fortunately, major high-consequence accidents in the nuclear weapons complex are rare and have not occurred for decades. Notwithstanding that good performance, DOE needs to continuously strive for (1) excellence in nuclear safety standards, (2) a proactive safety attitude, (3) world-class science and technology, (4) reliable operations of defense nuclear facilities, (5) adequate resources to support nuclear safety, (6) rigorous performance assurance, and (7) public trust and confidence. Safely managing the enduring nuclear weapon stockpile, fulfilling nuclear material stewardship responsibilities, and disposing of nuclear waste are missions with a horizon far beyond current experience and therefore demand a unique management structure. It is not clear that DOE is thinking in these terms.

This report synthesizes suggestions for provoking innovations and new solutions that should satisfy the Board's Recommendation 2004-1 and can help DOE improve the safe management of nuclear programs. For example, a separation of responsibility is suggested to clearly define and fulfill DOE's role as federal nuclear safety governance authority and its programmatic role to execute mission functions. Creation of a centralized nuclear safety function with well-defined authorities and experienced technical capabilities may resolve many of the issues identified by the Board. The ideas in this report are intended to promote a sustained organizational shift that should provide better balance between productivity and safety.

## TABLE OF CONTENTS

Section	Page
<b>1. INTRODUCTION .....</b>	<b>1-1</b>
<b>2. ORGANIZATIONAL SAFETY: BACKGROUND .....</b>	<b>2-1</b>
2.1 Normal Accident Theory .....	2-1
2.2 High-Reliability Organization Theory .....	2-2
2.3 Facility Safety Attributes .....	2-3
2.4 The Naval Reactors Program .....	2-5
<b>3. LESSONS LEARNED FROM RELEVANT ACCIDENTS .....</b>	<b>3-1</b>
3.1 Past Relevant Accidents .....	3-1
3.2 Recent Relevant Accidents .....	3-3
<b>4. DOE'S NUCLEAR SAFETY FOUNDATIONS .....</b>	<b>4-1</b>
<b>5. IDEAL ORGANIZATIONAL ATTRIBUTES .....</b>	<b>5-1</b>
<b>6. SUMMARY OF PUBLIC HEARINGS .....</b>	<b>6-1</b>
6.1 DOE's Proposed Safety Management Changes .....	6-1
6.2 Summary Evaluation of DOE Initiatives .....	6-5
<b>7. BOARD'S EVALUATION OF DOE .....</b>	<b>7-1</b>
7.1 Assessment of Safety Attributes .....	7-1
7.2 Discussion of Key Issues .....	7-8
<b>8. CONCLUSION .....</b>	<b>8-1</b>
8.1 The Board's Recommendation 2004-1 .....	8-1
8.2 Suggestions for Improvement .....	8-2
<b>APPENDIX: CHRONOLOGY OF KEY EVENTS IN DOE NUCLEAR SAFETY .....</b>	<b>A-1</b>
<b>REFERENCES .....</b>	<b>R-1</b>
<b>GLOSSARY OF ACRONYMS AND TERMS .....</b>	<b>GL-1</b>

## 1. INTRODUCTION

Many of the Department of Energy's (DOE) national security and environmental management programs are complex, tightly coupled systems<sup>1</sup> with high-consequence safety hazards. Mishandling of special nuclear materials and radiotoxic wastes can result in catastrophic events such as uncontrolled criticality, nuclear materials dispersal, and even inadvertent nuclear detonations. Simply stated, high-consequence nuclear accidents are not acceptable.

Major high-consequence accidents in the nuclear weapons complex are rare. DOE attempts to base its safety performance upon a foundation of defense in depth, redundancy, robust technical capabilities, large-scale research and testing, and nuclear safety requirements specified in DOE directives and rules. In addition, DOE applies the common-sense guiding principles and safety management functions of Integrated Safety Management (ISM)<sup>2</sup> (U.S. Department of Energy, 1996). Unfortunately, organizations that have not experienced high-consequence accidents may begin to question the value of rigorous safety compliance and tend to relax safety oversight, requirements, and technical rigor to focus on productivity. While the primary objective of any organizational safety management system is to prevent accidents so that individuals are not harmed and the environment is not damaged, organizational practices and priorities—especially those that emphasize efficiency—can potentially increase the likelihood of a high-consequence, low-probability accident.

In public hearings, DOE officials have reported that DOE is on a course to modify contracts so as to improve productivity and efficiency without degrading safety. The proposed changes are threefold. First, performance-based contracts are being designed to provide significant financial incentives for delivering on schedule and within budget, with apparent disincentives for failures to achieve performance measures. Second, to simplify its line management oversight processes, DOE will delegate to its field elements more contract authority and responsibility for negotiating and approving high-level performance measures, as well as assessing contractor compliance with requirements and safety performance. Third, DOE contractors will be expected to establish comprehensive self-assessment programs to monitor and evaluate all work performed under their contracts.

The Defense Nuclear Facilities Safety Board (Board) understands that contracts must reward effective program delivery, but emphasizing productivity can unintentionally lead to a reduced emphasis on safety. Likewise, comprehensive assessment close to where the work is being done makes sense, but assessments at all levels are needed for complete safety assurance. Finally, rigorous and credible contractor self-assessment is an important element of good safety management, but it does not obviate the need for DOE oversight.

---

<sup>1</sup> Complex, tightly coupled systems comprise numerous connected and interacting parts that react quickly to completion; once started, they can be stopped only with great difficulty, if at all. A nuclear weapon is clearly a complex, tightly coupled system.

<sup>2</sup> ISM is an overarching system developed to ensure that work is performed safely according to accepted controls. ISM can and should be applied at the activity, facility, and organization levels.

DOE officials have also reported that the Office of Independent Oversight and Performance Assurance will continue to periodically check the effectiveness of contractor and DOE field management assessment programs, and DOE headquarters will continue to issue nuclear safety directives and mission requirements. In concept, the changes will lead to a triad of oversight, starting with a foundation of contractor self-assessment, followed by site office monitoring of contractor performance, and independent sampling by headquarters of the effectiveness of contractor operations and site assessments. More emphasis will be placed on improving contractor self-assessment and less on centralized independent oversight. Two questions remain, however: Will the changes improve or diminish safety, and will the likelihood of the rare but catastrophic events that can occur in complex, tightly coupled operations increase, remain the same, or decrease?

The above proposed changes are part of a decades-old pendulum swing in the efforts of DOE and its predecessor organizations to balance safety and productivity. During the early part of the Cold War era, a consolidated body of safety information did not exist. Safety was based primarily on the experience of technical experts, with few regulations and little safety oversight. Productivity in building up the stockpile was high; however, risks were uncomfortably high, and environmental insults were considerable. The situation changed in the late 1980s for many reasons, not the least of which was the beginning of the end of the Cold War. Oversight during this period was initiated by “tiger team” audits; prescriptive regulations began to be enforced in the weapons complex; oversight was frequent and disorganized; and contractors had difficulty in implementing changing requirements. Meanwhile, demand from the Department of Defense ebbed. As a result, productivity plummeted while safety risks decreased, not just because of better safety practices, but also because little more was being accomplished.

At the urging of the Board (Recommendation 95-2, *Safety Management*), DOE and others realized the futility of this approach, and a common-sense method of integrating safety and work emerged. ISM was introduced as a standards-based, hazard-mitigation approach to working safely. Both DOE and its contractors worked to develop ISM, and to an extent, they have been successful. For DOE, however, the maturity of ISM systems remains mixed, while for contractors, issues related to implementation of ISM at the activity level persist.

DOE’s latest initiative builds on ISM, but gives more responsibility and flexibility to DOE field offices and contractors. The new approach is intended to increase productivity, but could move nuclear operations closer to a high-consequence accident. The underlying concern is that the pendulum may swing away from safety: decisions on balancing productivity and safety will be primarily in the hands of the contractors, independent DOE oversight will decrease, and risks to the public and workers could increase. This is clearly not an acceptable outcome.

This report explores some organizational aspects of safe operations, with the intent of helping to identify how DOE could better organize itself to enhance safety, particularly nuclear safety. The importance of organizational issues for safety was made clear in the report of the Columbia Accident Investigation Board (2003, Chapter 7). The ideal safety attributes and ideas for improvement presented in this report are offered in the spirit of providing background information and provoking ideas for implementing the Board’s Recommendation 2004-1, *Oversight of Complex, High-Hazard Nuclear Operations*.



Following this introduction, academic research on organizations involved in operations with the potential for high-consequence accidents and lessons learned from major accidents and near-misses are summarized (Sections 2 and 3, respectively). The foundations for nuclear safety within DOE are then described (Section 4). This is followed by the delineation of a set of organizational attributes for safely managing operations that can lead to high-consequence, low-probability accidents (Section 5). The report then describes DOE's proposed safety management changes and explains why the Board regards those changes as cause for concern (Section 6). Next, the organizational attributes set forth in Section 4 are applied to evaluate DOE's safety management of its high-hazard operations (Section 7). Finally, suggested improvements to DOE's safety management of these operations are presented (Section 8); those suggested actions have been provided to DOE as part of Recommendation 2004-1. In addition, the appendix presents a chronology of key events leading to the current state of DOE's Environment, Safety, and Health (ES&H) programs.

## 2. ORGANIZATIONAL SAFETY: BACKGROUND

### 2.1 NORMAL ACCIDENT THEORY

Organizational experts have analyzed the safety performance of high-risk organizations, and two opposing views of safety management systems have emerged. One viewpoint—normal accident theory,<sup>3</sup> developed by Perrow (1999)—postulates that accidents in complex, high-technology organizations are inevitable. Competing priorities, conflicting interests, motives to maximize productivity, interactive organizational complexity, and decentralized decision making can lead to confusion within the system and unpredictable interactions with unintended adverse safety consequences. Perrow believes that interactive complexity and tight coupling make accidents more likely in organizations that manage dangerous technologies. According to Sagan (1993, pp. 32–33), interactive complexity is “a measure . . . of the way in which parts are connected and interact,” and “organizations and systems with high degrees of interactive complexity . . . are likely to experience unexpected and often baffling interactions among components, which designers did not anticipate and operators cannot recognize.” Sagan suggests that interactive complexity can increase the likelihood of accidents, while tight coupling can lead to a normal accident. Nuclear weapons, nuclear facilities, and radioactive waste tanks are tightly coupled systems with a high degree of interactive complexity and high safety consequences if safety systems fail. Perrow’s hypothesis is that, while rare, the unexpected will defeat the best safety systems, and catastrophes will eventually happen.

Snook (2000) describes another form of incremental change that he calls “practical drift.” He postulates that the daily practices of workers can deviate from requirements for even well-developed and (initially) well-implemented safety programs as time passes. This is particularly true for activities with the potential for high-consequence, low-probability accidents. Operational requirements and safety programs tend to address the worst-case scenarios. Yet most day-to-day activities are routine and do not come close to the worst case; thus they do not appear to require the full suite of controls (and accompanying operational burdens). In response, workers develop “practical” approaches to work that they believe are more appropriate. However, when off-normal conditions require the rigor and control of the process as originally planned, these practical approaches are insufficient, and accidents or incidents can occur. According to Reason (1997, p. 6), “[a] lengthy period without a serious accident can lead to the steady erosion of protection . . . . It is easy to forget to fear things that rarely happen . . . .”

The potential for a high-consequence event is intrinsic to the nuclear weapons program. Therefore, one cannot ignore the need to safely manage defense nuclear activities. Sagan supports his normal accident thesis with accounts of close calls with nuclear weapon systems. Several authors, including Chiles (2001), go to great lengths to describe and analyze

---

<sup>3</sup> The terms “normal accident” and “organizational accident” are often used to describe the complex, unpredictable, perhaps unforeseeable events that can lead to the high-consequence accidents which are the focus of this paper. The Board uses the terms “normal accident” and “organizational accident” interchangeably throughout this paper to describe these events.

catastrophes—often caused by breakdowns of complex, high-technology systems—in further support of Perrow’s normal accident premise. Fortunately, catastrophic accidents are rare events, and many complex, hazardous systems are operated and managed safely in today’s high-technology organizations. The question is whether major accidents are unpredictable, inevitable, random events, or can activities with the potential for high-consequence accidents be managed in such a way as to avoid catastrophes. An important aspect of managing high-consequence, low-probability activities is the need to resist the tendency for safety to erode over time, and to recognize near-misses at the earliest and least consequential moment possible so operations can return to a high state of safety before a catastrophe occurs.

## 2.2 HIGH-RELIABILITY ORGANIZATION THEORY

An alternative point of view maintains that good organizational design and management can significantly curtail the likelihood of accidents (Rochlin, 1996; LaPorte, 1996; Roberts, 1990; Weick, 1987). Generally speaking, high-reliability organizations are characterized by placing a high cultural value on safety, effective use of redundancy, flexible and decentralized operational decision making, and a continuous learning and questioning attitude. This viewpoint emerged from research by a University of California-Berkeley group that spent many hours observing and analyzing the factors leading to safe operations in nuclear power plants, aircraft carriers, and air traffic control centers (Roberts, 1990). Proponents of the high-reliability viewpoint conclude that effective management can reduce the likelihood of accidents and avoid major catastrophes if certain key attributes characterize the organizations managing high-risk operations. High-reliability organizations manage systems that depend on complex technologies and pose the potential for catastrophic accidents, but have fewer accidents than industrial averages.

Although the conclusions of the normal accident and high-reliability organization schools of thought appear divergent, both postulate that a strong organizational safety infrastructure and active management involvement are necessary—but not necessarily sufficient—conditions to reduce the likelihood of catastrophic accidents. The nuclear weapons, radioactive waste, and actinide materials programs managed by DOE and executed by its contractors clearly necessitate a high-reliability organization. The organizational and management literature is rich with examples of characteristics, behaviors, and attributes that appear to be required of such an organization. The following is a synthesis of some of the most important such attributes, focused on how high-reliability organizations can minimize the potential for high-consequence accidents:

- *Extraordinary technical competence*—Operators, scientists, and engineers are carefully selected, highly trained, and experienced, with in-depth technical understanding of all aspects of the mission. Decision makers are expert in the technical details and safety consequences of the work they manage.
- *Flexible decision-making processes*—Technical expectations, standards, and waivers are controlled by a centralized technical authority. The flexibility to decentralize

operational and safety authority in response to unexpected or off-normal conditions is equally important because the people on the scene are most likely to have the current information and in-depth system knowledge necessary to make the rapid decisions that can be essential. Highly reliable organizations actively prepare for the unexpected.

- *Sustained high technical performance*—Research and development is maintained, safety data are analyzed and used in decision making, and training and qualification are continuous. Highly reliable organizations maintain and upgrade systems, facilities, and capabilities throughout their lifetimes.
- *Processes that reward the discovery and reporting of errors*—Multiple communication paths that emphasize prompt reporting, evaluation, tracking, trending, and correction of problems are common. Highly reliable organizations avoid organizational arrogance.
- *Equal value placed on reliable production and operational safety*—Resources are allocated equally to address safety, quality assurance, and formality of operations as well as programmatic and production activities. Highly reliable organizations have a strong sense of mission, a history of reliable and efficient productivity, and a culture of safety that permeates the organization.
- *A sustaining institutional culture*—Institutional constancy (Matthews, 1998, p. 6) is “the faithful adherence to an organization’s mission and its operational imperatives in the face of institutional changes.” It requires steadfast political will, transfer of institutional and technical knowledge, analysis of future impacts, detection and remediation of failures, and persistent (not stagnant) leadership.

## 2.3 FACILITY SAFETY ATTRIBUTES

Organizational theorists tend to overlook the importance of engineered systems, infrastructure, and facility operation in ensuring safety and reducing the consequences of accidents. No discussion of avoiding high-consequence accidents is complete without including the facility safety features that are essential to prevent and mitigate the impacts of a catastrophic accident. The following facility characteristics and organizational safety attributes of nuclear organizations are essential complements to the high-reliability attributes discussed above (American Nuclear Society, 2000):

- A robust design that uses established codes and standards and embodies margins, qualified materials, and redundant and diverse safety systems.
- Construction and testing in accordance with applicable design specifications and safety analyses.

- Qualified operational and maintenance personnel who have a profound respect for the reactor core and radioactive materials.
- Technical specifications that define and control the safe operating envelope.
- A strong engineering function that provides support for operations and maintenance.
- Adherence to a defense-in-depth safety philosophy to maintain multiple barriers, both physical and procedural, that protect people.
- Risk insights derived from analysis and experience.
- Effective quality assurance, self-assessment, and corrective action programs.
- Emergency plans protecting both on-site workers and off-site populations.
- Access to a continuing program of nuclear safety research.
- A safety governance authority that is responsible for independently ensuring operational safety.

These attributes are implemented at DOE in several ways. DOE has developed a strong base of nuclear facility directives, and authorizes operation of its nuclear facilities under regulatory requirements embodied in Title 10, Code of Federal Regulations, Part 830 (10 CFR Part 830), *Nuclear Safety Management* (2004). Part A of the rule requires contractors to conduct work in accordance with an approved quality assurance plan that meets established management, performance, and assessment criteria. Part B of the rule requires the development of a safety basis that (1) provides systematic identification of hazards associated with the facility; (2) evaluates normal, abnormal, and accident conditions that could contribute to the release of radioactive materials; (3) derives hazard controls necessary to ensure adequate protection of workers, the public, and the environment; and (4) defines the safety management programs necessary to ensure safe operations.

External oversight of nuclear safety is the responsibility of the Board,<sup>4</sup> an independent organization within the Executive Branch charged with overseeing public health and safety issues at DOE defense nuclear facilities. The Board reviews and evaluates the content and implementation of health and safety standards, as well as other requirements, relating to the design, construction, operation, and decommissioning of DOE's defense nuclear facilities. The Board ensures that those facilities are designed, built, and operated to established codes and standards that are embodied in rules and DOE directives.

---

<sup>4</sup> The Board provides independent oversight of DOE's defense nuclear facilities. The Board identifies safety issues before they become serious accidents, and influences change with action-forcing recommendations. The Board does not regulate, license, or enforce nuclear safety.

## 2.4 THE NAVAL REACTORS PROGRAM

There are several existing examples of high-reliability organizations. For example, Naval Reactors (a joint DOE/Navy program) has an excellent safety record, attributable largely to four core principles: (1) technical excellence and competence, (2) selection of the best people and acceptance of complete responsibility, (3) formality and discipline of operations, and (4) a total commitment to safety. Approximately 80 percent of Naval Reactors headquarters personnel are scientists and engineers. These personnel maintain a highly stringent and proactive safety culture that is continuously reinforced among long-standing members and entry-level staff. This approach fosters an environment in which competence, attention to detail, and commitment to safety are honored. Centralized technical control is a major attribute, and the 8-year tenure of the Director of Naval Reactors leads to a consistent safety culture. Naval Reactors headquarters has responsibility for both technical authority and oversight/auditing functions, while program managers and operational personnel have line responsibility for safely executing programs. “Too” safe is not an issue with Naval Reactors management, and program managers do not have the flexibility to trade safety for productivity. Responsibility for safety and quality rests with each individual, buttressed by peer-level enforcement of technical and quality standards. In addition, Naval Reactors maintains a culture in which problems are shared quickly and clearly up and down the chain of command, even while responsibility for identifying and correcting the root cause of problems remains at the lowest competent level. In this way, the program avoids institutional hubris despite its long history of highly reliable operations.

*NASA/Navy Benchmarking Exchange* (National Aeronautics and Space Administration and Naval Sea Systems Command, 2002) is an excellent source of information on both the Navy’s submarine safety (SUBSAFE) program and the Naval Reactors program. The report points out similarities between the submarine program and NASA’s manned spaceflight program, including missions of national importance; essential safety systems; complex, tightly coupled systems; and both new design/construction and ongoing/sustained operations. In both programs, operational integrity must be sustained in the face of management changes, production declines, budget constraints, and workforce instabilities. The DOE weapons program likewise must sustain operational integrity in the face of similar hindrances.

### **3. LESSONS LEARNED FROM RELEVANT ACCIDENTS**

#### **3.1 PAST RELEVANT ACCIDENTS**

This section reviews lessons learned from past accidents relevant to the discussion in this report. The focus is on lessons learned from those accidents that can help inform DOE's approach to ensuring safe operations at its defense nuclear facilities.

##### **3.1.1 Challenger, Three Mile Island, Chernobyl, and Tokai-Mura**

Catastrophic accidents do happen, and considering the lessons learned from these system failures is perhaps more useful than studying organizational theory. Vaughan (1996) traces the root causes of the Challenger shuttle accident to technical misunderstanding of the O-ring sealing dynamics, pressure to launch, a rule-based launch decision, and a complex culture. According to Vaughan (1996, p. 386), "It was not amorally calculating managers violating rules that were responsible for the tragedy. It was conformity." Vaughan concludes that restrictive decision-making protocols can have unintended effects by imparting a false sense of security and creating a complex set of processes that can achieve conformity, but do not necessarily cover all organizational and technical conditions. Vaughan uses the phrase "normalization of deviance" to describe organizational acceptance of frequently occurring abnormal performance.

The following are other classic examples of a failure to manage complex, interactive, high-hazard systems effectively:

- In their analysis of the Three Mile Island nuclear reactor accident, Cantelon and Williams (1982, p. 122) note that the failure was caused by a combination of mechanical and human errors, but the recovery worked "because professional scientists made intelligent choices that no plan could have anticipated."
- The Chernobyl accident is reviewed by Medvedev (1991), who concludes that solid design and the experience and technical skills of operators are essential for nuclear reactor safety.
- One recent study of the factors that contributed to the Tokai-Mura criticality accident (Los Alamos National Laboratory, 2000) cites a lack of technical understanding of criticality, pressures to operate more efficiently, and a mind-set that a criticality accident was not credible.

These examples support the normal accident school of thought (see Section 2) by revealing that overly restrictive decision-making protocols and complex organizations can result in organizational drift and normalization of deviations, which in turn can lead to high-consequence accidents. A key to preventing accidents in systems with the potential for high-consequence accidents is for responsible managers and operators to have in-depth technical

understanding and the experience to respond safely to off-normal events. The human factors embedded in the safety structure are clearly as important as the best safety management system, especially when dealing with emergency response.

### **3.1.2 USS Thresher and the SUBSAFE Program**

The essential point about United States nuclear submarine operations is not that accidents and near-misses do not happen; indeed, the loss of the USS Thresher and USS Scorpion demonstrates that high-consequence accidents involving those operations have occurred. The key point to note in the present context is that an organization that exhibits the characteristics of high reliability learns from accidents and near-misses and sustains those lessons learned over time—illustrated in this case by the formation of the Navy’s SUBSAFE program after the sinking of the USS Thresher. The USS Thresher sank on April 10, 1963, during deep diving trials off the coast of Cape Cod with 129 personnel on board. The most probable direct cause of the tragedy was a seawater leak in the engine room at a deep depth. The ship was unable to recover because the main ballast tank blow system was underdesigned, and the ship lost main propulsion because the reactor scrambled.

The Navy’s subsequent inquiry determined that the submarine had been built to two different standards—one for the nuclear propulsion-related components and another for the balance of the ship. More telling was the fact that the most significant difference was not in the specifications themselves, but in the manner in which they were implemented. Technical specifications for the reactor systems were mandatory requirements, while other standards were considered merely “goals.”

The SUBSAFE program was developed to address this deviation in quality. SUBSAFE combines quality assurance and configuration management elements with stringent and specific requirements for the design, procurement, construction, maintenance, and surveillance of components that could lead to a flooding casualty or the failure to recover from one. The United States Navy lost a second nuclear-powered submarine, the USS Scorpion, on May 22, 1968, with 99 personnel on board; however, this ship had not received the full system upgrades required by the SUBSAFE program. Since that time, the United States Navy has operated more than 100 nuclear submarines without another loss. The SUBSAFE program is a successful application of lessons learned that helped sustain safe operations and serves as a useful benchmark for all organizations involved in complex, tightly coupled hazardous operations.

The SUBSAFE program has three distinct organizational elements: (1) a central technical authority for requirements, (2) a SUBSAFE administration program that provides independent technical auditing, and (3) type commanders and program managers who have line responsibility for implementing the SUBSAFE processes. This division of authority and responsibility increases reliability without impacting line management responsibility. In this arrangement, both the “what” and the “how” for achieving the goals of SUBSAFE are specified and controlled by technically competent authorities outside the line organization. The implementing organizations are not free, at any level, to tailor or waive requirements



unilaterally. The Navy's safety culture, exemplified by the SUBSAFE program, is based on (1) clear, concise, non-negotiable requirements; (2) multiple, structured audits that hold personnel at all levels accountable for safety; and (3) annual training.

## **3.2 RECENT RELEVANT ACCIDENTS**

Two recent events—the near-miss at the Davis-Besse Nuclear Power Station and the Columbia space shuttle disaster—continue to support normal accident theory. Lessons learned from both events have been thoroughly analyzed (Columbia Accident Investigation Board, 2003; Travers, 2002), so the comments here are limited to insights gained at public hearings held by the Board on the impact of DOE's oversight and management practices on the health and safety of the public and workers at DOE's defense nuclear facilities.

### **3.2.1 The Nuclear Regulatory Commission and the Davis-Besse Incident**

The Nuclear Regulatory Commission (NRC) was established in 1974 to regulate, license, and provide independent oversight of commercial nuclear energy enterprises. While NRC is the licensing authority, licensees have primary responsibility for safe operation of their facilities. Like the Board, NRC has as its primary mission to protect the public health and safety and the environment from the effects of radiation from nuclear reactors, materials, and waste facilities. Similar to DOE's current safety strategy, NRC's strategic performance goals include making its activities more efficient and reducing unnecessary regulatory burdens. A risk-informed process is used to ensure that resources are focused on performance aspects with the highest safety impacts. NRC also completes annual and for-cause inspections, and issues an annual licensee performance report based on those inspections and results from prioritized performance indicators. NRC is currently evaluating a process that would give licensees credit for self-assessments in lieu of certain NRC inspections. Despite the apparent logic of NRC's system for performing regulatory oversight, the Davis-Besse Nuclear Power Station was considered the top regional performer until the vessel head corrosion problem described below was discovered.

During inspections for cracking in February 2002, a large corrosion cavity was discovered on the Davis-Besse reactor vessel head. Based on previous experience, the extent of the corrosive attack was unprecedented and unanticipated. More than 6 inches of carbon steel was corroded by a leaking boric acid solution, and only the stainless steel cladding remained as a pressure boundary for the reactor core. In May 2002, NRC chartered a lessons-learned task force (Travers, 2002). Several of the task force's conclusions that are relevant to DOE's proposed organizational changes were presented at the Board's public hearing on September 10, 2003.

The task force found both technical and organizational causes for the corrosion problem. Technically, a common opinion was that boric acid solution would not corrode the reactor vessel head because of the high temperature and dry condition of the head. Boric acid leakage was not considered safety-significant, even though there is a known history of boric acid attacks in

reactors in France. Organizationally, neither the licensee self-assessments nor NRC oversight had identified the corrosion as a safety issue. NRC was aware of the issues with corrosion and boric acid attacks, but failed to link the two issues with focused inspection and communication to plant operators. In addition, NRC inspectors failed to question indicators (e.g., air coolers clogging with rust particles) that might have led to identifying and resolving the problem. The task force concluded that the event was preventable had the reactor operator ensured that plant safety inspections received appropriate attention, and had NRC integrated relevant operating experiences and verified operator assessments of safety performance. It appears that the organization valued production over safety, and NRC performance indicators did not indicate a problem at Davis-Besse. Furthermore, licensee program managers and NRC inspectors had experienced significant changes during the preceding 10 years that had depleted corporate memory and technical continuity.

Clearly, the incident resulted from a wrong technical opinion and incomplete information on reactor conditions and could have led to disastrous consequences. Lessons learned from this experience continue to be identified (U.S. General Accounting Office, 2004), but the most relevant for DOE is the importance of (1) understanding the technology, (2) measuring the correct performance parameters, (3) carrying out comprehensive independent oversight, and (4) integrating information and communicating across the technical management community.

### 3.2.2 Columbia Space Shuttle Accident

The organizational causes of the Columbia accident received detailed attention from the Columbia Accident Investigation Board (2003) and are particularly relevant to the organizational changes proposed by DOE. Important lessons learned (National Nuclear Security Administration, 2004) and examples from the Columbia accident are detailed below:

- **High-risk organizations can become desensitized to deviations from standards**—In the case of Columbia, because foam strikes during shuttle launches had taken place commonly with no apparent consequence, an occurrence that should not have been acceptable became viewed as normal and was no longer perceived as threatening. The lesson to be learned here is that oversimplification of technical information can mislead decision makers.

In a similar case involving weapon operations at a DOE facility, a cracked high-explosive shell was discovered during a weapon dismantlement procedure. While the workers appropriately halted the operation, high-explosive experts deemed the crack a “trivial” event and recommended an unreviewed procedure to allow continued dismantlement. Presumably the experts—based on laboratory experience—were comfortable with handling cracked explosives, and as a result, potential safety issues associated with the condition of the explosive were not identified and analyzed according to standard requirements. An expert-based culture—which is still embedded in the technical staff at DOE sites—can lead to a “we have always done things that way and never had problems” approach to safety.

- **Past successes may be the first step toward future failure**—In the case of the Columbia accident, 111 successful landings with more than 100 debris strikes per mission had reinforced confidence that foam strikes were acceptable.

Similarly, a glovebox fire occurred at a DOE closure site where, in the interest of efficiency, a generic procedure was used instead of one designed to control specific hazards, and combustible control requirements were not followed. Previously, hundreds of gloveboxes had been cleaned and discarded without incident.

Apparently, the success of the cleanup project had resulted in management complacency and the sense that safety was less important than progress. The weapons complex has a 60-year history of nuclear operations without experiencing a major catastrophic accident;<sup>5</sup> nevertheless, DOE leaders must guard against being conditioned by success.

- **Organizations and people must learn from past mistakes**—Given the similarity of the root causes of the Columbia and Challenger accidents, it appears that NASA had forgotten the lessons learned from the earlier shuttle disaster.

DOE has similar problems. For example, release of plutonium-238 occurred in 1994 when storage cans containing flammable materials spontaneously ignited, causing significant contamination and uptakes to individuals. A high-level accident investigation, recovery plans, requirements for stable storage containers, and lessons learned were not sufficient to prevent another release of plutonium-238 at the same site in 2003. Sites within the DOE complex have a history of repeating mistakes that have occurred at other facilities, suggesting that complex-wide lessons-learned programs are not effective.

- **Poor organizational structure can be just as dangerous to a system as technical, logistical, or operational factors**—The Columbia Accident Investigation Board concluded that organizational problems were as important a root cause as technical failures. Actions to streamline contracting practices and improve efficiency by transferring too much safety authority to contractors may have weakened the effectiveness of NASA's oversight.

DOE's currently proposed changes to downsize headquarters, reduce oversight redundancy, decentralize safety authority, and tell the contractors "what, not how" are notably similar to NASA's pre-Columbia organizational safety philosophy. Ensuring safety depends on a careful balance of organizational efficiency, redundancy, and oversight.

---

<sup>5</sup> A major fire in 1957 at a Rocky Flats plutonium facility that resulted in the release of significant amounts of plutonium was the closest system-level accident in the DOE weapons complex.

- **Leadership training and system safety training are wise investments in an organization's current and future health**—According to the Columbia Accident Investigation Board, NASA's training programs lacked robustness, teams were not trained for worst-case scenarios, and safety-related succession training was weak. As a result, decision makers may not have been well prepared to prevent or deal with the Columbia accident.

DOE leaders role-play nuclear accident scenarios, and are currently analyzing and learning from catastrophes in other organizations. However, most senior DOE headquarters leaders serve only about 2 years, and some of the site office and field office managers do not have technical backgrounds. The attendant loss of institutional technical memory fosters repeat mistakes. Experience, continual training, preparation, and practice for worst-case scenarios by key decision makers are essential to ensure a safe reaction to emergency situations.

- **Leaders must ensure that external influences do not result in unsound program decisions**—In the case of Columbia, programmatic pressures and budgetary constraints may have influenced safety-related decisions.

Downsizing of the workload of the National Nuclear Security Administration (NNSA), combined with the increased workload required to maintain the enduring stockpile and dismantle retired weapons, may be contributing to reduced federal oversight of safety in the weapons complex. After years of slow progress on cleanup and disposition of nuclear wastes and appropriate external criticism, DOE's Office of Environmental Management initiated "accelerated cleanup" programs. Accelerated cleanup is a desirable goal—eliminating hazards is the best way to ensure safety. However, the acceleration has sometimes been interpreted as permission to reduce safety requirements. For example, in 2001, DOE attempted to reuse 1950s-vintage high-level waste tanks at the Savannah River Site to store liquid wastes generated by the vitrification process at the Defense Waste Processing Facility to avoid the need to slow down glass production. The first tank leaked immediately. Rather than removing the waste to a level below all known leak sites, DOE and its contractor pursued a strategy of managing the waste in the leaking tank, in order to minimize the impact on glass production.

- **Leaders must demand minority opinions and healthy pessimism**—A reluctance to accept (or lack of understanding of) minority opinions was a common root cause of both the Challenger and Columbia accidents.

In the case of DOE, the growing number of "whistle blowers" and an apparent reluctance to act on and close out numerous assessment findings indicate that DOE and its contractors are not eager to accept criticism. The recommendations and feedback of the Board are not always recognized as helpful. Willingness to accept criticism and diversity of views is an essential quality for a high-reliability organization.

- **Decision makers stick to the basics**—Decisions should be based on detailed analysis of data against defined standards. NASA clearly knows how to launch and land the space shuttle safely, but somehow failed twice.

The basics of nuclear safety are straightforward: (1) a fundamental understanding of nuclear technologies, (2) rigorous and inviolate safety standards, and (3) frequent and demanding oversight. The safe history of the nuclear weapons program was built on these three basics, but the proposed management changes could put these basics at risk.

- **The safety programs of high-reliability organizations do not remain silent or on the sidelines; they are visible, critical, empowered, and fully engaged**—Workforce reductions, outsourcing, and loss of organizational prestige for safety professionals were identified as root causes for the erosion of technical capabilities within NASA.

Similarly, downsizing of safety expertise has begun in NNSA's headquarters organization, while field organizations such as the Albuquerque Service Center have not developed an equivalent technical capability in a timely manner. As a result, NNSA's field offices are left without an adequate depth of technical understanding in such areas as seismic analysis and design, facility construction, training of nuclear workers, and protection against unintended criticality. DOE's ES&H organization, which historically had maintained institutional safety responsibility, has now devolved into a policy-making group with no real responsibility for implementation, oversight, or safety technologies.

- **Safety efforts must focus on preventing instead of solving mishaps**—According to the Columbia Accident Investigation Board (2003, p. 190), "When managers in the Shuttle Program denied the team's request for imagery, the Debris Assessment Team was put in the untenable position of having to prove that a safety-of-flight issue existed without the very images that would permit such a determination. This is precisely the opposite of how an effective safety culture would act."

Proving that activities are safe before authorizing work is fundamental to ISM. While DOE and its contractors have adopted the functions and principles of ISM, the Board has on a number of occasions noted that DOE and its contractors have declared activities ready to proceed safely despite numerous unresolved issues that could lead to failures or suspensions of subsequent readiness reviews.

#### 4. DOE'S NUCLEAR SAFETY FOUNDATIONS

DOE's current nuclear safety program has evolved during years of change in leadership, missions, organizational structure, and statutory requirements. Under the terms of the Atomic Energy Act of 1954, as amended, DOE has the authority and responsibility for governing its nuclear activities to ensure protection of the public and workers from exposure to radioactive materials and for safeguarding its special nuclear materials. The Appendix provides a brief background on nuclear weapon safety programs to provide a historical perspective on the current reengineering proposals.

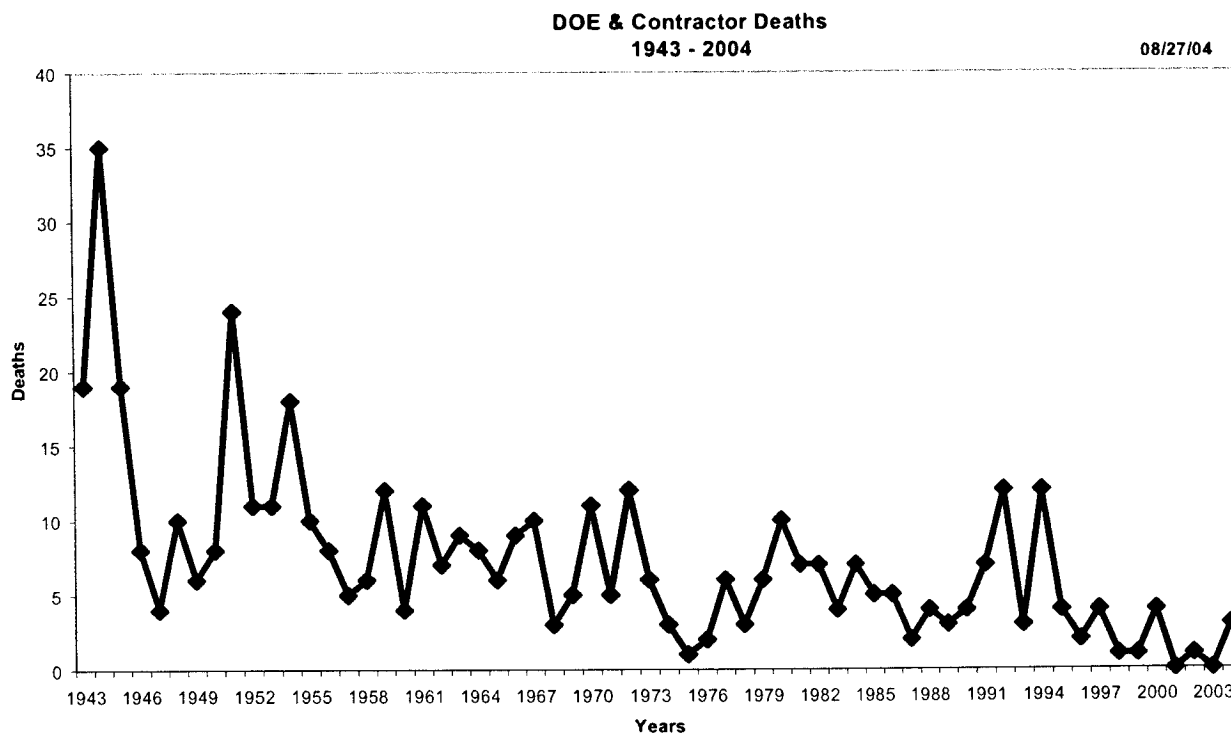
In summary, DOE's ES&H program is a complex, overlapping collection of regulations, contractual requirements, and guidance. Responsibility for the various safety functions is dispersed, the headquarters organization has become a bureaucracy, and central leadership changes frequently. Nevertheless, major high-consequence accidents at DOE are rare. One explanation for this is that DOE's safety foundation has been (and should continue to be) based on defense in depth, redundancy, robust technical capabilities, large-scale research and testing, and nuclear safety requirements specified in DOE directives and rules. In addition, DOE has introduced the common-sense guiding principles and safety management functions of ISM.

At the urging of the Board (Recommendation 95-2, *Safety Management*), DOE adopted the concept of ISM as its reference approach to safety management. ISM is based on standards for identifying and controlling hazards to ensure that work is done safely. Through departmental policies, rules, and contract terms, DOE has defined expectations relative to safety practices for its contractors. Primary responsibility for safety lies with line managers. Federal employees, who are assigned mission responsibilities, also ensure that the contractors comply with safety requirements. DOE codified quality assurance and facility safety basis requirements in 10 CFR Part 830. As ISM was implemented, DOE directives were revised so that only a relatively small set of high-level safety expectations remained in the orders and manuals. Other safety requirements and guidance from previous orders were transferred to guides and standards. The intent under this system is for DOE's contractors and contracting officers to use a standards and requirements identification process to select a set of binding safety requirements that will be graded to the work at contract sites.

The success of the concept of ISM depends on its proper implementation. This includes ensuring that roles and responsibilities are clearly defined and that implementing mechanisms, such as procedures, are developed for the discharge of those roles and responsibilities. For DOE and some contractors, effecting this has required a level of formality that in many places did not exist. Difficulty has been experienced in defining roles and responsibilities, and the development of mechanisms has been mixed.

Fatalities from all accidents across the entire DOE complex from the Manhattan Project to August 31, 2004, are plotted in Figure 4-1, which shows that the evolution of DOE's safety foundation has improved protection for workers at nuclear sites during the last 60 years. The vast majority of these accidental deaths were related to transportation, construction, and industrial accidents; only four deaths are attributable to radiation. Furthermore, since the Rocky

Flats fire in 1969 the defense nuclear programs have not experienced a catastrophic, system-level accident of the magnitude of the Challenger, Three Mile Island, or the USS Thresher. While uncertainty cannot be eliminated, it appears that the likelihood of fatalities and catastrophic nuclear accidents can be reduced through rigorous attention to the fundamentals of safety management systems. Attention, particularly at the federal level, to ensuring that ISM is properly implemented and executed will enhance DOE's ability to become a high-reliability organization.



**Figure 4-1. Accidental Fatalities from DOE's Defense Nuclear Activities**

## 5. IDEAL ORGANIZATIONAL ATTRIBUTES

Notwithstanding DOE's past safety record, one must note that responsibilities related to the various safety functions that ensure safe operations are not always apparent, nor are they being managed at the federal level as an integrated whole. DOE has adopted the ISM concept to bring stability to its safety management program, but losses of technical expertise at headquarters, coupled with the relatively rapid turnover of key administrators and pressures to reduce budgets and staffs, have given rise to organizational changes in functions and responsibilities that are not in the best interests of safety. The following discussion highlights important organizational attributes that DOE should pursue and retain despite influences to the contrary.

The background information on complex, high-hazard activities presented in the preceding sections sets the stage for identifying an optimum set of primary attributes and secondary characteristics needed to safely manage DOE's nuclear weapons, nuclear materials, and nuclear waste operations. At the highest level, DOE should establish and maintain excellence in nuclear safety standards, a proactive safety attitude, world-class science and technology, reliable operations and nuclear facilities, adequate resources to support nuclear safety, rigorous performance assurance metrics, and public trust and confidence. The most important attributes, from the Board's perspective, are in the following functional areas:

- **Safety Standards**—Clear, concise technical safety directives based on sound engineering fundamentals that are centrally developed, controlled, and verified form an essential foundation for ensuring safe nuclear operations. These directives comprise stringent quality assurance, nuclear safety bases, safety management, and radiation protection standards. In addition, nuclear facilities must be built on the basis of robust designs, engineered safety features, and defense in depth using codes and standards that clearly control the safe operating envelope.
- **Safety Attitude**—A fundamental principle of a good safety attitude is the need to prove that there is *no* unaddressed safety problem before work begins. Senior leaders need to be committed equally to the value of safety and productivity and not give mixed signals about the importance of safety. A questioning attitude and constructive skepticism that challenges conclusions need to be encouraged at all levels of the organization.
- **Technical Excellence**—Technical excellence denotes that safety analyses are based on sound engineering judgment grounded in a solid science foundation, including physics, chemistry, and nuclear technologies. Personnel have in-depth understanding of both safety and technical aspects of the mission, and the organization sustains a focus on nuclear safety research and testing. Risk-informed decisions are derived from test results, analysis, and experience.



- **Operational Excellence**—Robust nuclear facility safety systems are independent, redundant, and diverse, but not overly complex. Defense in depth is designed into nuclear facilities, and safety margins are carefully maintained. Operating hazards are controlled to prevent or mitigate accidents, and safety is embedded in processes and procedures through a functioning formal safety management system.
- **Safety Resources**—Safety issues must have equal status with productivity in funding and schedule priorities. Resources should be available for safety upgrades and repairs to aging infrastructure. Modern infrastructure is maintained, and new facility construction is started as needed. There should be sufficient organizational redundancy to manage and oversee safety performance independently.
- **Performance Assurance**—Competent, robust, frequent, and centralized oversight is a foundation for excellence in performance assurance. Readiness is verified before hazardous operations commence. A performance assurance program is established to predict and prevent accidents, using realistic performance indicators and trend analysis. Rapid response to problems and closeout of issues can ensure that small issues do not become large ones.
- **Public Trust**—Public trust is maintained by having a compelling mission that respects public safety, sustained through continuity of key technical officials. Also necessary are credible and effective external oversight, a positive safety attitude, information-sharing programs, and the strong presence of stakeholders.

Section 7 of this report presents the Board’s assessment of the performance of DOE’s centralized organization as compared with the above attributes relative to managing activities with the potential for high-consequence accidents.

## **6. SUMMARY OF PUBLIC HEARINGS**

This section describes the safety management changes proposed by DOE during the Board's public hearings and provides the Board's summary evaluation of those initiatives.

### **6.1 DOE'S PROPOSED SAFETY MANAGEMENT CHANGES**

The overarching initiatives presented by DOE officials at the Board's public hearings involve efforts to improve efficiency and lower costs so that more work can be accomplished. Specifically, the reengineering effort is centered on three approaches: (1) develop incentives that motivate contractors to complete mission-related tasks, (2) remove obstacles perceived as constraining contractors trying to complete mission-related tasks by streamlining requirements, and (3) reduce costs by eliminating redundancy and cutting back the size of the federal workforce. These three approaches are discussed in turn below.

#### **6.1.1 Develop Incentives That Motivate Contractors**

An incentive-based contract strategy requires development and tracking of important performance measures. DOE's Assistant Secretary for ES&H touched on this point when she stated, "The biggest challenge is to understand the drivers of good behavior and unacceptable behavior. It is easy to just assume it is bad people or a bad company, but that is unrealistic. Other actions drive people and companies to do things that are fundamentally against their nature." However, actions that are unacceptable in hindsight are not necessarily the result of decisions that "go against an [organization's] nature." Undesirable outcomes can be the consequence of rational and conscious decision making. This is one of the drawbacks of relying excessively on performance-based contracts. The requirements allow for establishing clear accountability after an undesirable event, but are less useful in providing direction for avoiding such an event.

The concern about managing by incentives is particularly important in the area of nuclear safety, where it is difficult to develop reliable leading indicators that will warn of impending high-consequence accidents. Requirements that there be "no organizational accidents," "no criticality accidents," or "adequate protection of the workers" broadly capture DOE's objectives, but are untenable as a governance scheme because the evidence of a violation involves the unacceptable condition that was to be avoided. Performance metrics, such as lost work days or reportable incidents, can be misleading and can actually increase the likelihood of a high-consequence accident if controls and oversight are relaxed in response to a system that appears to be in control and improving. Almost all of the senior DOE officials who testified at the Board's public hearings appeared to be applying this false logic, as the following statements attest:

We believe that ISM has improved safety performance by ensuring that line and facility managers are directly involved in and responsible and accountable for

safety management. The benefits of this approach are seen through a review of various performance metrics, such as a downward trend in injury and illness rates at our facilities. (Deputy Secretary of Energy, October 21, 2003)

The Department's safety performance clearly shows our ability to get more work done and do it safer. The DOE injury and illness rates have declined to a historic low in 2003. (Under Secretary of Energy, Science, and Environment, November 21, 2003)

The Office of Independent Oversight and Performance Assurance has noted that ISM programs are maturing and are having a demonstrable positive impact on safety. We have seen improving trends in worker injury rates and environmental compliance performance metrics. (Director of Independent Oversight and Performance Assurance, October 21, 2003)

The Assistant Secretary for ES&H described a more complete process for evaluating performance metrics: "I believe the Department has evolved in its ability to track and trend safety performance at the corporate level. ES&H not only looks at the 'numbers,' but we also want to understand exactly what is driving certain performance. A site may have good TRC [total recordable case] and LWC [lost workday case] rates, but if near-misses are occurring at an increased rate, we need to understand why and ensure line management takes corrective actions." This statement has merit, but it still refers to conclusions drawn from existing, albeit conflicting, data. It does not recognize that the lack of negative data is not a sound basis for making judgments about organizational accidents. However, the Assistant Secretary also alluded to an effort to rely more on performance data to determine when safety issues require more explicit government involvement in contractor activities: "The act of measuring, in and of itself, will drive performance. People will pay attention to what you measure. Over time, an organization should be able to identify precursor indications that lead to unacceptable events, and be able to monitor those indicators rather than being event driven."

Measuring performance is important, and many DOE performance measures, particularly for individual (as opposed to organizational) accidents, show rates that are low and declining further. However, the Assistant Secretary's statement can be interpreted to indicate that DOE plans to transition to a system of monitoring precursor events to determine when conditions have degraded such that action is necessary to prevent an accident. Indicators can inform managers that conditions are degrading, but it is inappropriate to infer that the risk of a high-consequence, low-probability accident is acceptable based on the lack of "precursor indications." In fact, the important lesson learned from the Davis-Besse event is not to rely too heavily on this type of approach (see Section 3.2.1).

### 6.1.2 Streamline Requirements

DOE's second approach to improving efficiency and lowering costs relates to the specification of DOE requirements and expectations. As described in the Appendix, DOE and its predecessor agencies have developed a body of requirements and guidance during the last 60 years that captures the experience of the nuclear industry. This body of safety standards extends from very broad and high-level policy guidance to very narrowly focused and prescriptive guidance on how to design a specific component or conduct a particular task.

DOE made a major change in its safety governance scheme during the mid-1990s. On the basis of extensive and detailed reviews, orders and manuals were reduced to contain only high-level safety expectations, which are generally applicable to most of DOE's defense nuclear work. More explicit "how-to" or process-related direction was extracted and placed in guides and standards. The structure of DOE's directives system implies that many or most of the safety expectations set forth in orders and manuals should be included in contract requirements. Directives issued as guides or standards are presumably intended to be optional or replaceable by equivalent industry standards. The core safety practices retained in rules, orders, and manuals, which have evolved over the years in response to lessons learned, are expected to remain relatively constant and be changed only for cause.

The current trend is to continue to minimize requirements that are either inapplicable, insufficiently tailored, or too prescriptive. The Deputy Secretary testified, "The Department has continued its multiyear focus on improving its requirements by removing overly prescriptive, redundant, and conflicting requirements where possible. However, the primary principle in our efforts to streamline requirements has been and remains that DOE requirements must ensure adequate safety." The Assistant Secretary for ES&H described the issues even more directly:

There have been many initiatives over the last few years to better set requirements. It has been recognized that DOE's requirements are sometimes confusing, conflicting, and not properly applied. Even with the advent of our current contracting method, where the set of applicable requirements are negotiated and documented in the contract, the contracts often contained requirements that were not directly relevant to the work at hand. This has led to a system of waivers, exceptions, and inconsistent practices in holding contractors accountable for the items in their contracts.

Therefore, there has been an effort under way to streamline the requirements. The purpose is not to lower our standards for safety and performance, but rather to come to a concise, relevant set of requirements and then to hold contractors fully accountable for meeting those requirements . . . . Once the right requirements are identified, compliance should be strictly enforced.

As described above, there have been numerous efforts to streamline safety requirements and simplify the requirements tailoring process. Past initiatives have reduced and simplified the DOE directives for safety—perhaps too much. At a minimum, it no longer appears that DOE can gain substantially in productivity by reducing safety requirements without impacting safety. In addition, the proposed DOE model is that DOE contracting officers will start with a minimal set of safety requirements and, through negotiation with the contractor, add further requirements to arrive at an appropriate set. It is difficult to understand why DOE believes that the same people who were unsuccessful in eliminating unnecessary requirements will be more successful in adding them when necessary.

### **6.1.3 Reduce Costs by Eliminating Redundancy and Reducing the Workforce**

DOE is motivated to streamline its operations and reduce redundancy, including both redundant systems and programs, such as reporting of data, and layers of management and oversight. DOE is attempting to develop streamlined information and reporting systems that will keep federal employees aware of the status of operations by DOE contractors in all areas, such as finances, security, project realization, and safety, without requiring as much direct day-to-day involvement as there has been in the past. The Administrator for NNSA described the changes:

NNSA has placed primary responsibility for oversight in the hands of its Site Office Managers who have first-hand knowledge of our contractors' operations. These managers were chosen for their experience and ability, and have been given the responsibility for defining the organizations and hiring the staff required to accomplish their responsibilities. Additional technical expertise is also available to the Site Office Managers through the newly established Service Center.

The Administrator also described some aspects of NNSA's streamlining efforts: "Last year, as part of our streamlining efforts, I eliminated routine Headquarters on-site reviews. I believe that this was a correct decision and consistent with placing greater responsibility on our site offices. Nonetheless, we have this policy under continuous review and I will not hesitate to reinstate Headquarters reviews if necessary."

NNSA is seeking to reduce the redundancy in its decision making by delegating authority as far down the chain of command as possible (again with the asserted caveat of not compromising safety). The logic is that the people closest to the work being performed (i.e., the site office managers and the individual site contractors) have the most intimate knowledge of the safety issues involved; therefore, they will make the best decisions. This logic has merit, but there are some assumptions inherent in this model that need to be explicitly discussed.

One assumption is that NNSA will place competent individuals in these key site office manager positions. The NNSA Administrator has already acknowledged this point and has expressed at the Board's hearings his intent to put high-quality managers at the sites. This may not be sufficient, however. The complexity and variety of the issues facing DOE exceed the

ability of even a brilliant scientist or engineer to master. It is important that strong site office managers also have highly competent staff in sufficient numbers and of appropriate skills to support them. This point was also recognized by NNSA officials, who informed the Board that all of the site office managers have asserted that they can complete their missions with the number of personnel assigned to them. However, recent actions by some NNSA site office managers suggest that they realize their initial assessments were overly optimistic. For example, NNSA has taken steps to increase the number of personnel at the Pantex Site Office and Los Alamos Site Office.

Another assumption imbedded in NNSA's shift to decentralized operations is that the activities at each NNSA site are sufficiently unique that an individual solution to most safety issues will be more efficient than any economy of scale gained by having centralized authority and common requirements. However, unacceptable, high-consequence nuclear accidents such as criticality, radioactive material dispersal, and inadvertent nuclear detonation are not site-specific. These potential accidents have common initiating events. Therefore, a common set of requirements would reduce the likelihood of such events.

Still another assumption holds that the site offices have mature, well-defined processes in place to discharge their roles and responsibilities. This capability is particularly important for delegated roles and responsibilities. In these instances, the person delegating the function must require objective evidence that the site office has the capability and capacity to execute the delegation. In terms of oversight, this should include a site office oversight or assessment procedure that has been used to demonstrate that a given contractor has a robust self-assessment program.

A final assumption is that once responsibility has been transferred successfully to the contractors and performance metrics are in place, fewer people will be required to oversee performance metrics. This assumption depends on the site contractors performing rigorous self-assessments. However, the Director of the Office of Independent Oversight and Performance Assurance testified at the Board's public hearings that "contractor assurance programs still vary in effectiveness and, for the most part, are not yet sufficiently robust, rigorous, and self-critical to warrant reductions in DOE line management oversight."

A complication involved in this approach is that DOE is not just the customer for the goods and services produced by its contractors; it is also the owner of most of the facilities in which the contractor operates. DOE must accept liability for the results of its contractors' work (e.g., the environmental, health, and safety implications, as well as security and financial implications). This means that DOE must accept the consequences of the methods chosen by the contractors to fulfill their missions even if it did not specify or control those methods.

## **6.2 SUMMARY EVALUATION OF DOE INITIATIVES**

The initiatives described above have improved productivity. DOE contractors are becoming more productive; Environmental Management sites are making progress on cleanup of legacy wastes and decommissioning of nuclear facilities; and NNSA's weapons complex has

increased output in the areas of surveillance, testing, manufacturing, stockpile downsizing, and nuclear material processing activities in support of national security missions. However, pressure to increase productivity and reduce costs continues. The concern is that changes to relax requirements and achieve high productivity can increase the likelihood of a catastrophic accident. This is not DOE's intent, and DOE senior managers assert that no changes will be made that will reduce safety to an unacceptable level. Assertions and intentions aside, however, it is not possible to judge absolutely the safety condition of complex, tightly coupled systems. All that can be said with confidence is that the current trend makes a high-consequence, low-probability accident more likely than it was before.

DOE is motivated to achieve efficiency and productivity, cost savings, and improved performance (including safety performance) through innovation. Many believe that DOE's traditional management, contracting, and governance structure limits the creativity and innovation DOE seeks to foster. The belief is that DOE has become too prescriptive and/or invasive in its approach and has specified requirements that are either inappropriate for the work at hand or not as efficient as other alternatives. As the Deputy Secretary of Energy said in his testimony to the Board, "We use performance-based contracts to encourage innovation, to ensure progress towards goals, and to promote cost-effective approaches." Likewise, the NNSA Administrator stated, "We believe reengineering is solving critical problems involving confused accountability, stovepiping, and pervasive micro-management. At the same time, as we implement these changes, I am committed to ensuring no reduction in the effectiveness of our safety oversight."

DOE's approach to these ends involves relying on market forces and the creativity of its contractors to drive change. DOE's solution to this problem is to focus more precisely on what programs are trying to achieve, specify those goals clearly and succinctly so that contractors know exactly what is expected of them, measure results to determine whether expectations are being fulfilled, and then reward or penalize contractors based on their performance. Contractors will be told "what" is required of them but not "how" to achieve it. The belief is that if this approach is properly implemented, the contractors' decision making will be in line with the government's interests and will be more creative, effective, and efficient.

The first challenge acknowledged by DOE is to devise contracts and incentive structures that will align the contractors' interests with those of the government. The current contracting model at DOE is to maximize competition in part by increasing the frequency of contract rebids. This means that generally DOE contractors are limited to a 5-year planning horizon. In some cases, such as environmental restoration or cleanup contracts, that time frame is consistent with the length of DOE's interests as owner, customer, and self-governor. In other instances, however, such as facilities and technical capabilities needed to support the enduring nuclear weapon stockpile, sites that will store nuclear materials for decades, and repositories that will store nuclear wastes for centuries, the government's period of interest is much longer than a 5-year contract. In such cases, it is difficult to devise a system whereby contract incentives alone, with only minimal DOE involvement in decisions about "how" to achieve the mission, will lead a short-term, for-profit contractor to make business decisions entirely consistent with the government's interests. Safely managing the nation's nuclear weapons and fulfilling nuclear

materials stewardship responsibilities are missions with a horizon far beyond any contract experience and therefore demand a unique management structure. It is not clear that DOE is thinking in these terms.

The potential negative consequences of the proposed efficiency improvements are without doubt contrary to the intent and direction provided by senior DOE leaders. However, such reengineering initiatives can also reduce the feedback available to these managers such that undesired conditions can exist without their knowledge.



## **7. BOARD'S EVALUATION OF DOE**

### **7.1 ASSESSMENT OF SAFETY ATTRIBUTES**

Based on the research in the field, testimony provided at the Board's public meetings, and the personal experience of the Board and its staff, the Board developed a model of key attributes that DOE should have in its role as owner, customer, and governor of hazardous nuclear activities. The Board began by identifying the desired attributes of organizations that are responsible for hazardous operations. The Board then used the functional areas delineated in Section 5 to focus and organize these attributes. One of those areas, public trust, is not directly related to the ability of DOE to minimize the potential for an organizational accident; in fact, DOE's success in developing the desired attributes in the other six areas will have a direct influence on the public's trust in DOE to execute its missions safely. Within each of the six remaining functional areas, the Board listed the key attributes that are necessary to achieve excellence in that area. These attributes include concepts that are related to high-reliability organizations, but they are specific to nuclear weapons and related missions.

The Board then assessed the performance of DOE against these attributes to look for trends and to identify common areas in need of additional attention. The Board started by reviewing the testimony and written statements provided by DOE and contractor personnel during the Board's public hearings to determine how DOE assessed its own performance in each of these areas. Because the Board's model was developed after the series of public meetings, DOE did not address all of the attributes directly or even indirectly, and in some cases there was no consensus among the many DOE and contractor personnel about DOE's performance in a particular area. Nevertheless, the Board did discern clear patterns of strengths and weaknesses from DOE's self-perceptions. The Board then reviewed DOE's directives to evaluate how well they set out plans, processes, and guidance to institutionalize the attributes of high-reliability organizations in the Board's model. In general, the Board found most of the attributes discussed at some level in the DOE directives, although many were covered only superficially. Finally, the Board evaluated DOE's implementation of each attribute based on the Board's experience in overseeing DOE's nuclear operations and concluded if the intent of each attributes was substantially met, partially met, or needs improvement. The results of applying this assessment tool are reported in Section 7.1.7 below.

The fundamental value of the Board's evaluation model was not in the value assigned to each individual element, but in the search for patterns and areas where DOE could focus to maximize its efforts to improve safety. The results of the Board's evaluation helped the Board formulate the specific subrecommendations in Recommendation 2004-1, *Oversight of Complex, High-Hazard Nuclear Operations*.

### **7.1.1 Safety Standards**

The Board concluded that DOE has a good set of safety standards to serve as the basis for specifying and controlling its hazardous nuclear activities, although this set of standards should be more centrally controlled. Lack of central control has led to implementation problems—specifically, deviations in practice from written expectations. The Board also concluded that DOE’s objective to streamline its safety standards is inhibiting continuous improvement in the standards in areas where new, additional requirements are needed. At the facility and activity levels, DOE has established technical specifications that control the safe operation of its defense nuclear facilities in the form of documented safety analyses and technical safety requirements, which are now in place for many of those facilities. However, formal authorization agreements between DOE and its contractors that clearly specify operating requirements have not always been kept up to date.

The Board also considered clear and documented organizational roles and responsibilities to be a safety standard. DOE has a corporate Functions, Responsibilities, and Authorities Manual that flows down into similar documents for subtier organizations. However, these documents are in a constant state of flux, and thus actual roles, responsibilities, and authorities are often in question. This situation creates confusion in the flowdown to implementing mechanisms and procedures, resulting in a wide range of formality for a given office. Expectations for how federal staff formally discharge their responsibilities should be part of implementing a rigorous ISM program.

### **7.1.2 Safety Attitude**

In general, the Board has observed that DOE’s senior leaders express a consistent commitment to safety. However, decisions made by these leaders do not always demonstrate equal value placed on safety and productivity. One of the significant manifestations of this contradiction is that DOE has not yet established a culture of timely and comprehensive communication of safety issues. At the activity level, the Board concluded that DOE and contractor personnel believe they have the authority and responsibility to stop unsafe work. DOE has not yet achieved a more proactive culture in which people adhere to safety standards while maintaining a questioning attitude, and workers establish the fact that hazards are controlled before starting work. A potentially worrisome deviation from a good safety attitude is the tendency of DOE and its contractors to be lulled into complacency, and even arrogance, based on past successes.

### **7.1.3 Technical Excellence**

DOE has a solid foundation of science and engineering, particularly in its laboratories, although this expertise is not always available when and where it is needed, and the capability and capacity to address safety issues are lacking in the federal workforce. Strong technical capability is particularly lacking at the more senior levels of DOE. The problem of degrading

technical competence among DOE and its contractors is becoming more severe because senior leaders have not focused on recruiting, retaining, and training outstanding technical personnel and then placing them in positions of authority. Nor has DOE given adequate attention to the need for safety-focused research. At the facility and activity levels, DOE has not maintained adequate technical quality and rigor in its safety analyses and in its facility and system designs. Increasingly, the quality of many of these intellectual products is being achieved only through exhaustive review and revision cycles and intervention by the Board. The Board believes that the increasing number of problems with the original submissions of safety analyses, technical safety requirements, and design documents is an indication of the declining technical ability of DOE and its contractors.

#### **7.1.4 Operational Excellence**

DOE has made progress in the implementation of ISM. Increasingly, personnel in the field identify hazards, establish controls, and operate in accordance with procedures. One particular recurring safety problem is that DOE often attempts to start new operations or restart existing operations before the activity has achieved an adequate level of safety performance.

#### **7.1.5 Safety Resources**

In recent years, DOE has generally not provided all the resources necessary to ensure reliably safe operation of high-hazard activities. These include financial resources for replacing or refurbishing old facilities and equipment, ensuring adequate design margins and quality for safety in new facilities and equipment, and hiring technical safety experts. Problems with safety resources extend as well to not allowing time in project schedules for training, testing, and qualification of both people and equipment. Resources are also required in the form of authority and influence for safety professionals in the organization and redundancy within the organization itself to ensure the identification, reporting, and resolution of safety issues.

#### **7.1.6 Performance Assurance**

The Board concluded that DOE does not have a robust performance assurance capability. Current independent assessments are carried out by a relatively small staff whose reviews cannot have the necessary breadth and depth to be relied upon as the sole basis for independent assessment of DOE's safety performance. More significant, DOE's line organizations do not adequately use self-assessments to identify issues, determine root causes, develop solutions, and resolve issues to prevent their recurrence. Despite this situation, there have been initiatives to reduce the number or limit the scope of DOE independent and self-assessments of safety in the complex.

### 7.1.7 Summary of the Board's Assessment

The information below summarizes the Board's assessment of DOE against the key attributes within each of the above six functional areas. As noted, each attribute is assessed as substantially met, partially met, or needs improvement. Overall, the number of attributes that need improvement or are only partially met suggests that DOE needs to improve its ability to conduct its mission safely. In fact, NNSA's Columbia Accident Investigation Board Lessons Learned Review team stated, "NNSA exhibits technical capability and organizational problems similar to those identified by the Columbia Accident Investigation Board" (National Nuclear Security Administration, 2004). The same could be said of DOE as a whole. Many of the attributes listed below can be directly linked to the guiding principles and core functions of ISM; thus a secondary conclusion is the possibility that DOE has lost direction in fully implementing and executing ISM. This in turn may indicate that there are unclear expectations for federal personnel regarding the level of formality needed to fully implement ISM, and that a better understanding in this area may need to be inculcated.

#### Safety Standards

- Clear, concise technical safety directives that are centrally developed and controlled, and are based on sound engineering judgment and data—**partially met**.
- Technical specifications clearly control the safe operating envelope—**substantially met**.
- Stringent quality assurance, safety management, and radiological protection requirements—**substantially met**.
- Clear roles, responsibilities, and authorities; clear organizational structure and lines of authority—**partially met**.
- Deviations from technical standards are rare, compelling, and approved centrally—**needs improvement**.
- Formal facility authorization agreements between owner and operator—**partially met**.
- Continuously improve safety standards and practices through lessons learned and safety research—**needs improvement**.

#### Safety Attitude

- Prove that there is no safety problem before starting work—**partially met**.
- Senior leaders are committed to the mission and are drivers of safety, especially nuclear safety—**partially met**.

- Rigorous adherence to safety standards and regulations—**partially met**.
- Equal value of safety and productivity—**needs improvement**.
- Workers at any level can stop unsafe work—**substantially met**.
- Question deviances, and avoid institutional complacency or arrogance based on past successes—**needs improvement**.
- Senior managers continuously stress safety of operations and individual accountability for safety—**needs improvement**.
- Encourage a questioning attitude and constructive skepticism; challenge conclusions—**needs improvement**.
- Safety and its ownership are apparent in everyone's actions and deeds—**partially met**.
- Respect for radioactive materials, criticality, and other hazards associated with nuclear activities—**partially met**.
- Timely and unfiltered alerts of problems and credible operational information through multiple paths of communication—**partially met**.
- Self-reporting encouraged, and identification of safety errors/failures rewarded—**partially met**.
- Strong sense of mission with balanced production and defined safety goals—**needs improvement**.

### **Technical Excellence**

- Robust facility designs using established codes and standards—**partially met**.
- Safety analysis based on sound engineering judgment and data—**partially met**.
- Defense in depth designed into nuclear facilities, including independent, redundant, and diverse safety systems that are not overly complex—**partially met**.
- Solid foundation of science and engineering, including physics, chemistry, and nuclear technologies—**substantially met**.
- Technical support personnel have expert-level technical understanding—**needs improvement**.

- Senior managers have strong technical backgrounds—**partially met**.
- Recurrent and relevant training—**partially met**.
- Continuing focus on nuclear safety research and testing—**needs improvement**.
- Embedded technical and safety expertise—**needs improvement**.
- High priority on recruiting, selection, and retention of technical staff—**needs improvement**.
- Complete system knowledge allows prompt anticipation or investigation of system problems—**partially met**.
- Personnel have in-depth understanding of safety and technical aspects of job—**needs improvement**.
- Strong safety development and testing capability—**needs improvement**.
- Risk management tools integrated into decisions—**needs improvement**.
- Seek to identify safety problems that are not known or expected—**needs improvement**.

### **Operational Excellence**

- Hazards are controlled to prevent or mitigate accidents—**partially met**.
- Adherence to technical procedures (or stopping and correcting procedure) is a fundamental expectation—**partially met**.
- Nuclear facility construction follows rigorous quality assurance, configuration management, and safety practices—**partially met**.
- Systems and equipment maintained in accordance with the facility design basis—**partially met**.
- Managers maintain awareness of operational conditions/issues—**partially met**.
- Operations are prepared and ready to operate safely prior to independent readiness reviews—**needs improvement**.
- Readiness verified before starting hazardous work—**partially met**.

- Flexible response to off-normal and emergency events through relentless preparation and training—**partially met**.
- Safety embedded in processes and procedures through a functioning formal ISM system—**partially met**.
- Aggressive reporting and evaluation of occurrences, deviations, etc.—**partially met**.
- Decentralized operational authority during off-normal events—**substantially met**.
- Operations personnel held to a high standard of technical understanding, not just task-oriented training—**needs improvement**.
- Safety margins are carefully maintained—**needs improvement**.

### **Safety Resources**

- Safety issues and productivity carry equal weight for funding allocations and schedule flexibility—**needs improvement**.
- Resources available for safety upgrades and repairs to aging infrastructure—**partially met**.
- Continuity/constancy of key technical officials—**needs improvement**.
- Safety positions have adequate organizational influence—**needs improvement**.
- Sufficient redundancy in organizational safety functions—**needs improvement**.
- Modern infrastructure and new facility construction are funded—**partially met**.
- System of priority checks and balances from top to bottom—**partially met**.
- Independently funded safety research—**needs improvement**.

### **Performance Assurance**

- Robust, frequent, and independent oversight—**needs improvement**.
- DOE/NNSA managers actively involved in safety issues and performance assurance—**partially met**.
- Rapid response to problems and closeout of issues—**needs improvement**.

- High-quality root-cause analysis—**partially met.**
- Performance is tracked based on valid indicators and robust trend analysis—**needs improvement.**
- Performance oversight at all levels—**needs improvement.**
- Learn using a feedback and improvement program designed to capture industry-wide lessons—**needs improvement.**
- Readiness for high-risk activities verified by DOE/NNSA—**partially met.**
- Decentralized assessment and corrective action programs—**needs improvement.**
- Linkages among problems and organizational issues are examined—**partially met.**
- Centralized verification of compliance with safety and technical requirements—**needs improvement.**
- Robust assessment and corrective action programs, including effective tracking of issues—**needs improvement.**

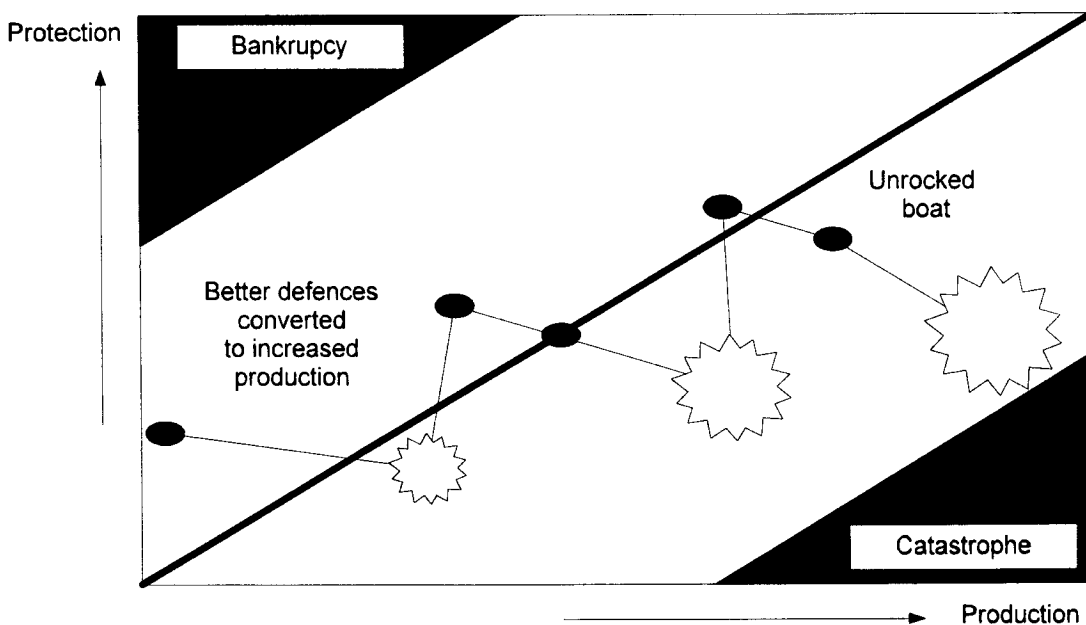
## 7.2 DISCUSSION OF KEY ISSUES

### 7.2.1 Balanced Priorities

Balancing the often competing priorities of safety and productivity is a management challenge that is crucial to avoiding high-consequence accidents while meeting mission requirements. One of the seven guiding principles of DOE's ISM system states that "resources shall be effectively allocated to address safety, programmatic, and operational considerations. Protecting the public, the workers, and the environment shall be a priority whenever activities are planned and performed" (U.S. Department of Energy, 1996, p. 2). Nevertheless, in the nuclear weapons and environmental management programs, safety and productivity compete for the same funding pool, and success in achieving high levels of safety is not always considered as valuable as meeting program expectations on schedule and within budget. Although excellence in safety performance is an implicit factor in project success, milestone completion is rewarded, while safety is recognized only when failures are punished. Sometimes line managers have to choose between safety and meeting deadlines. Potential for reward is often a stronger motivator than fear of punishment, so some decisions may not be as conservative from a safety perspective as prudence would dictate. In most cases, the decision to trade safety for productivity does not result in an actual accident. The "successful" outcome of such cases can breed complacency, and the result can be a gradual degradation of safety margins leading to a major accident.



Normal accident theory asserts that accidents in high-risk activities may occur unexpectedly (see Section 2.1). High-reliability organization theory describes the attributes of organizations that have achieved sustained operations without high-consequence accidents (see Section 2.2). Neither theory addresses how variations in the conduct of different organizations affect the likelihood of a normal accident. Reason (1997) provides a framework to integrate both of these concepts. He uses a hypothetical protection versus production operating space to help visualize the relationship between safety and productivity. Figure 7-1, from Reason's book, plots this hypothetical cycle, whereby an organization may relax safety protection controls to increase profits until an accident occurs, forcing management to impose greater protection, but resulting in reduced productivity. High-reliability organizations consistently exhibit characteristics and attributes that keep them predominantly on the side of the cycle where accidents are less likely to occur. However, these real-world organizations sometimes, even if only temporarily, drift to the less-safe side of the cycle, and even when they do not, they can experience a normal accident. Simply stated, too high an investment in protection can lead to a business failure, while too much risk taking can lead to a catastrophic accident. During times of high productivity and good safety performance, the investment in safety protection drops off. When an accident or near-miss attracts the attention of management, safety protection measures are strengthened. According to Reason, the cycle repeats itself after productivity falls off and operations once again appear to be safe, until a major system catastrophe ends the enterprise in failure.



**Figure 7-1. The Life Span of a Hypothetical Organization Through the Production—Protection Space.** (Source: Reason, 1997, p. 5. Reproduced with permission from the author.)

A cycle of productivity and event-driven safety reactions can be found in the history of the nuclear weapons program. The incredibly productive Manhattan Project was followed by an awareness of the health effects of radiation and the possibility of an inadvertent criticality event. The outcome was strict, expert-based guidelines for handling and radiation control of nuclear materials. Design and development of new nuclear weapons were accompanied by a period of atmospheric testing, which was subsequently banned when it was found that significant quantities of plutonium and fission products were being released to the environment. The rapid buildup of nuclear weapons during the Cold War led to environmental impacts from poorly controlled radioactive waste facilities. These unanticipated impacts led to stringent environmental controls and regulations imposed on the weapons program. Fifty years later, DOE is still working under the oversight regulations imposed by federal and state environmental agencies to clean up the radioactive residues from the weapons buildup.

A major building fire at Rocky Flats in 1969 led to an external radioactive release that basically shut down the operation and led to a plethora of requirements and regulations defining boundaries for nuclear materials handling activities. An increase in accidents, near-misses, and deaths at DOE sites during the mid-1980s led to enhanced oversight and rules and orders for hazard identification and work control. The 2000 forest fire that threatened Los Alamos National Laboratory led to improvements in emergency response and fire control. While it is not possible to quantify the impacts, it is worth considering whether the cycle is damping out the swings toward catastrophe or masking the possibility of a serious nuclear accident. For example, will DOE's accelerated cleanup activities or steps to decrease safety oversight encourage line managers to cut safety corners, leading to a gradual reduction in safety margins that could ultimately result in a major system failure in one of DOE's complex, high-hazard, tightly coupled systems?

### **7.2.2 Self-Assessment**

Having a strong program for assessment combined with responsive corrective actions is another fundamental tenet of effective safety management, the premise being that if the organization takes care of the small things, the big things will take care of themselves. DOE self-governs, self-measures, self-corrects, and self-enforces both the nuclear and industrial safety performance of the government-owned/contractor-operated nuclear weapons complex. Recent organizational changes are driving these functions for safety oversight farther down the government/contractor hierarchy, both to improve efficiency and to reduce the burden of unnecessary safety requirements.

The Institute of Nuclear Power Operations (1999, p. 3) has established principles for self-assessment to improve safety performance: "In highly effective organizations, managers and workers seek continuous improvement by identifying and implementing opportunities for improvement. In these organizations, the need for improvement is driven from within rather than by external factors or influences." Krause (1995) has developed an employee-driven safety assessment system that has successfully reduced incident and accident rates to very low levels by identifying and correcting leading indicators of poor safety practices. Clearly, contractor line

management must have primary responsibility for ensuring safe operations of nuclear facilities and for ensuring and maintaining safe work practices at the activity level. The nuclear power industry finds self-assessments to be a cost-effective way of improving safety performance; however, the continuity of rigorous self-assessments and incentives to identify issues must be carefully maintained by oversight agencies. An important incentive for effective self-assessment is effective external oversight, inspection, and enforcement.

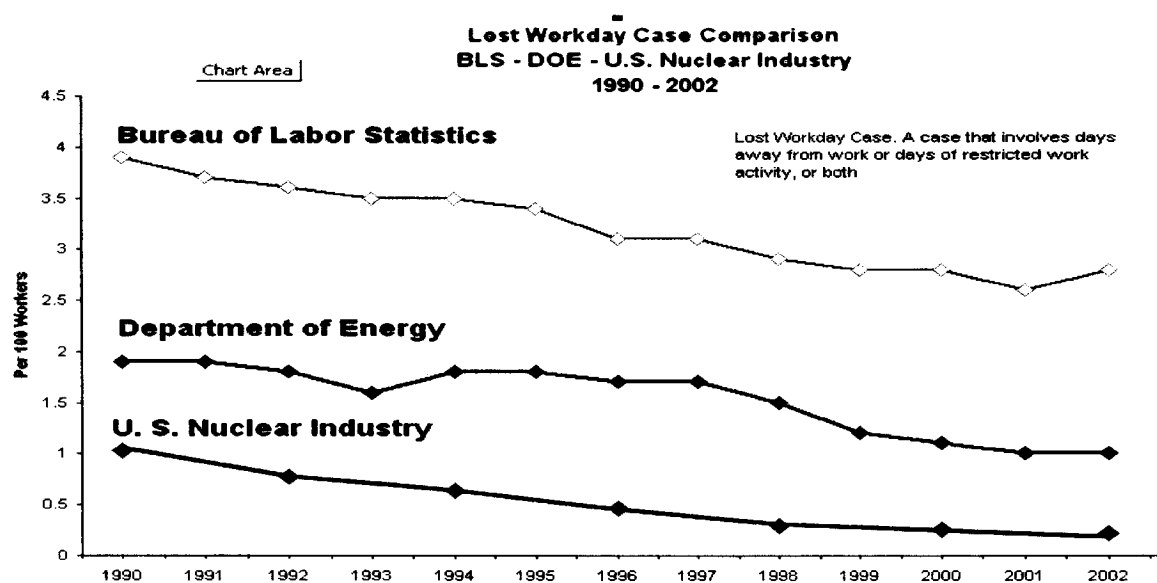
Similarly, in testimony before the Board, DOE officials claimed that assigning the responsibility for safety oversight to DOE field offices should enhance performance. Field office safety experts work nearer to the hazardous facilities, and presumably understand the hazards involved better than people at DOE headquarters. DOE's initiatives to reduce unnecessary safety requirements and redundant oversight through enhanced self-assessments represent key aspects of the productivity versus safety balance.

While the concepts are viable, is there objective evidence that DOE's field offices have properly implemented ISM? Do these site offices have mechanisms and procedures in place for critical functions such as self-assessment and assessment of their contractors? Has oversight reached a level of maturity at which increased reliance on contractor self-assessment is appropriate? Will reduced oversight and self-assessment decrease the likelihood of a high-consequence accident in high-hazard, complex organizations?

All of DOE's contracts have detailed performance indicators that require contractors to track, trend, and correct safety problems identified by self-assessment. Indeed, most indicators selected by DOE's contractors are showing measurable improvements, and it would be logical to conclude that an organization that performs well must be succeeding. However, self-assessment processes can miss significant problem conditions, as apparently happened with the deep corrosion in the Davis-Besse reactor pressure vessel head (see Section 3.2.1). There is the potential for self-assessments not to be as rigorous as independent external inspections and to inflate performance ratings (U.S. Department of Energy, 2003). In addition, how well past performance predicts future performance depends on the validity of the data, the random nature of accidents, and measurement of accurate predictive parameters. In the defense nuclear complex, the validity of DOE's reporting of occupational injuries is suspect (U.S. Department of Energy, 2004); catastrophic accidents in complex, tightly coupled systems are random, low-probability events; and one can certainly question the correlation between minor incidents and major nuclear accidents. Furthermore, it does not matter how well an organization is doing if failure is too costly to tolerate; in that case, leaders must protect the system from extraordinary events. Finally, too much reliance on self-assessment can lead to downplaying the importance of the independent and redundant oversight that is essential to operating a high-risk endeavor successfully.

### 7.2.3 Performance Measures

Measurable safety performance can be improved, as shown by the trends in Figure 7-2. DOE's performance data on reportable and lost workday cases reveal roughly half the national industrial average and have been showing a steady downward trend since 1990. While DOE's performance is better than national averages, however, the commercial nuclear industry has lower accident rates.



**Figure 7-2. Summary of Lost Workday Rates for U.S. Industry, DOE, and the Commercial Nuclear Industry, 1990–2002**

A potential misperception is to conclude that if the frequency of these types of accidents is declining, then the likelihood of high-consequence, low probability nuclear accidents is also declining. The assumption is that if human error can be eliminated, organizational safety will be ensured. However, this assertion denies random—some would say inevitable—events. The use of performance metrics, particularly those involving such data as lost workdays or reportable incidents, can be misleading and can actually increase the likelihood of a nuclear accident if controls and oversight are inappropriately relaxed in response to a system that appears to be in control and improving. As Reason (1997, p. 232) notes, “A low loss time injury rate reveals very little about the likelihood of an organizational accident.” For example, NASA’s safety performance prior to both the Challenger and Columbia accidents was excellent and clearly did not indicate an impending safety problem with launches. More recently, NNSA had judged Los Alamos National Laboratory’s handling of classified data to be satisfactory, but control of electronic media containing classified data was not properly maintained. This is not to suggest that tracking and correcting incidents is not valuable; in fact, experience with the Naval Reactors program (see Section 2.4) suggests that prompt reporting and correction of small problems will prevent big problems from occurring.

None of the above discussion is aimed at discrediting performance measures—they play an important role in improving safety. The point is not to be lulled into complacency by improvements in industrial safety performance.

## 8. CONCLUSION

Clearly the recent changes proposed and under way at DOE stem from important and desirable objectives. These efforts have improved performance in many areas and can be tied to some impressive increases in productivity. Additionally, DOE and contractor personnel have continued if not increased their stated emphasis on safety as their most important objective and their assurance that they will take no action that produces an unacceptable risk. However, emerging changes to DOE's organizational structure, staffing, oversight policies, and contracts could reduce defense in depth, decentralize safety authorities, reward productivity over safety, reduce key technical capabilities, and thereby create conditions in which a high-consequence event is more likely than it was before these initiatives were undertaken. The loss of expertise at DOE, the potential for people to inappropriately emphasize production over safety, the loss of awareness of events and deviations from accepted norms, the relaxation of vigilance, a shift from "proving an activity is safe" to "detecting if it becomes unsafe," a lack of a questioning attitude, and a reduction in visibility of dissenting opinions or contrary information—all of which are occurring to some extent at DOE—are correlated with increased risk of an organizational accident.

The question is how to safely and productively organize and manage defense nuclear activities that are inherently expensive and complex and for which the consequences of failure are significant. The likelihood of a nuclear accident can be reduced by identifying hazards, eliminating and/or controlling risks, and maintaining safety systems. Hazard identification and control, technical and operational excellence, and overarching nuclear safety standards, underpinned by adequate safety research and testing and overseen by centralized and independent safety assessments, appear to be the keys to effective safety management of nuclear operations. DOE has to develop its own organization within its legal, budgetary, and mission constraints. The ideal safety attributes and ideas for improvement presented in this report are offered in the spirit of providing background information and provoking ideas for implementing the Board's Recommendation 2004-1, *Oversight of Complex, High-Hazard Nuclear Operations*.

### 8.1 THE BOARD'S RECOMMENDATION 2004-1

As a result of testimony received at its public hearings, the Board issued three subrecommendations in Recommendation 2004-1, *Oversight of Complex, High-Hazard Nuclear Operations*. The Board's assessment of DOE's performance against ideal organizational attributes helped form the basis for this Recommendation. The correlation between the organizational attributes identified by the Board and the three subrecommendations is described below. The Board recommended:

1. That delegation of authority for nuclear safety matters to field offices and contractors be contingent upon the development and application of criteria and implementing mechanisms to ensure that:

- a) **oversight responsibility** includes the capability for examining, assessing, and auditing by all levels of the DOE organizations *[This subrecommendation is embodied in the specific attributes under Safety Attitude and Performance Assurance];*
  - b) the **technical capability** and appropriate experience for effective safety oversight are in place *[This subrecommendation is embodied in the specific attributes under Technical Excellence and Safety Resources];*
  - c) **corrective action plans** consistent with recommendations resulting from internal DOE reviews of the Columbia accident and the Davis-Besse incident are issued *[This subrecommendation is embodied in the specific attributes under Performance Assurance].*
2. That to ensure that any features of the proposed changes will not increase the likelihood of a low-probability, high-consequence nuclear accident, DOE take steps to:
- a) empower a **central** and technically competent **authority** responsible for operational and nuclear safety goals, expectations, requirements, standards, directives, and waivers *[This subrecommendation is embodied in the specific attributes under Safety Standards, Safety Attitude, and Technical Excellence];*
  - b) ensure the continued integration and support of **research, analysis, and testing** in nuclear safety technologies *[This subrecommendation is embodied in the specific attributes under Safety Resources and Technical Excellence];*
  - c) require that the principles of **Integrated Safety Management** serve as the foundation of the implementing mechanisms at the sites *[This subrecommendation is embodied in the specific attributes under Safety Standards and Operational Excellence].*
3. That direct and unbroken line of **roles and responsibilities** for the safety of nuclear operations—from the Secretary of Energy and the NNSA Administrator to field offices and sites—be insured according to appropriate Functions, Responsibilities, and Authorities documents and Quality Assurance Implementation Plans *[This subrecommendation is embodied in the specific attributes under Safety Standards].*

## 8.2 SUGGESTIONS FOR IMPROVEMENT

Recommendation 2004-1 and this report serve as background on what the problem is, what the state of the organization is, and what organizational elements need to improve to manage DOE's high-risk nuclear operations safely. Determining how to modify DOE's safety management systems is the job of DOE senior management and is the subject of the Implementation Plan for Recommendation 2004-1.

The Implementation Plan for Recommendation 2004-1 has to be mindful of the three simultaneous (and potentially conflicting) federal roles for conducting work at DOE's defense nuclear facilities.

1. As the *customer*, DOE focuses on the deliverables called for in its contracts. In this role, DOE's expectations are intended to define as clearly as possible the goods, services, and results that the government seeks. DOE's oversight as a customer is based on ensuring that high-quality deliverables are provided as efficiently and effectively as possible.
2. As the *owner* of nuclear facilities, DOE—the government's agent—retains responsibility for the accidents that occur at its facilities. Responsibility for accepting risk may be delegated to field offices, but senior leaders at DOE headquarters remain accountable.
3. As the *self-governor for nuclear safety*, DOE establishes nuclear safety expectations, monitors to see whether safety requirements are being satisfied, and enforces safety requirements with fines and penalties.

As a self-governing agency in the area of nuclear safety, DOE is obliged to fulfill several necessary functions: (1) developing and promulgating safety requirements, (2) imposing requirements on contractors and DOE program and line managers, (3) accepting or rejecting proposals for safety commitments of the governed entities, (4) conducting assessments to ensure that governed entities comply with the commitments in authorization agreements, and (5) enforcing compliance when violations of an authorization agreement are identified. As the owner of most of the facilities used to accomplish its nuclear-related mission, DOE must also fulfill the obligations of a governed entity. These functions include (1) conducting the analyses and committing to the controls, policies, and procedures necessary to satisfy nuclear safety requirements; (2) faithfully implementing safety commitments according to the authorization agreement; and (3) ensuring that contractors fulfill their safety requirements through effective oversight.

The Secretary of Energy is responsible for both DOE's governance and mission functions. However, DOE's roles and responsibilities as self-governor and customer/owner need to be clearly separated. The Board believes that the self-governance function should not be delegated below the level of the Under Secretary for Energy, Science, and Environment and the NNSA Administrator. In the DOE organization, the Assistant Secretary (Cognizant Secretarial Office/Program Secretarial Officer) level is the logical beginning of the "governed" portion of the line management chain of command. Therefore, while the Assistant Secretaries, the DOE field elements, and the contractors are responsible for nuclear safety *performance*, they should not have responsibility for nuclear safety *governance*. As currently organized, however, DOE provides no integrated, centralized control over these basic safety management functions.



With this fundamental organizational perspective in mind, the Board concludes that:

1. DOE needs to establish a central safety authority with the technical capability and capacity to oversee nuclear safety in a quality manner.
2. DOE needs to conduct safety research to support the central safety authority.
3. The Cognizant Secretarial Office and Program Secretarial Officer organizations, as the top of the “governed” portion of the line management chain, and subordinate organizations should focus on the implementation of quality assurance and safety management. This includes line oversight and awareness.

The following is a synthesis of suggestions for organizational improvements that should satisfy Recommendation 2004-1 and can help DOE enhance the safe management of nuclear weapons, actinide materials, and radioactive waste programs. These suggestions are not intended to represent the only ways of satisfying the Recommendation, but to provoke innovations and new solutions to the issues involved.

### **8.2.1 Central Authority**

Nuclear safety governance of defense nuclear activities should be retained at high levels of line management to ensure consistency in policies, requirements, interpretations, and decisions affecting the likelihood of a high-consequence accident. Such responsibilities should be held by managers who do not have the real or perceived conflict of simultaneously being responsible for the day-to-day performance of programmatic missions. Line managers at the Assistant Secretary level and below are responsible for day-to-day results of programmatic missions. Therefore, line managers above the Assistant Secretary level should retain the responsibility and authority for setting and enforcing nuclear safety requirements and function as the “central safety authority.”

Line managers at the Assistant Secretary level and below primarily fulfill DOE’s role as owner of DOE facilities, and should be given the responsibility and authority to achieve programmatic mission objectives consistent with the safety requirements established and administered at higher levels of the organization. This suggested action would preserve responsibility for operational decision making and for implementation of safety requirements at the DOE Assistant Secretary level and below and strengthen accountability to the ultimate line authority within DOE.

Responsibility and authority for nuclear safety goals, expectations, requirements, standards, directives, and waivers should reside at the Under Secretary level or above. The nuclear safety officers proposed in Section 8.2.2 would have responsibility for advising the Secretary, the Deputy Secretary, and/or the Under Secretaries on the technical standards required for nuclear facilities, exceptions to standards compliance, and safety research. The nuclear safety officers would be responsible for a final review of safety analysis reports, technical safety requirements, and authorization agreements for all nuclear facilities. In addition, they would

carry out, or at least contribute to, the headquarters independent oversight function, independently verify readiness to start high-hazard operations, and independently oversee the design and construction of nuclear facilities.

### **8.2.2 Oversight Responsibility**

Centralized oversight of safety performance at contractor-operated sites is one of the main functions of the owning agency. Because oversight redundancy, technical strength, and effective performance assurance may be weakening, the Board believes that this function requires immediate attention. While the Office of Independent Oversight and Performance Assurance and the Office of Price Anderson Enforcement are effective oversight groups, their oversight activities are infrequent and often reactive. Oversight by DOE programmatic and field offices and contractor self-assessment are necessary but not sufficient to fulfill all needed oversight roles. Oversight activities by the proposed central safety authority is also needed to ensure that the field is implementing safety requirements consistently, utilizing proactive performance measures, and implementing complex-wide lessons learned. This responsibility is best fulfilled through day-to-day awareness of issues and decisions made by the programmatic line organizations rather than large, process-focused periodic reviews. The objective is to prevent accidents instead of reacting after the fact. Free-access, hands-on, and independent safety oversight of the nuclear activities of Environmental Management and NNSA should be a functional responsibility of the Under Secretary for Energy, Science and Environment (ESE) and the NNSA Administrator.

Because these top line management positions are normally short in tenure, it would be necessary to create senior, highly placed career nuclear safety officers in ESE and NNSA with staffs of technical experts in all major safety disciplines. A primary function of the safety officer would be to prevent the “practical drift” that slowly moves work toward less rigorous safety practices.

### **8.2.3 Nuclear Safety Research**

DOE needs to secure adequate resources (money, people, and time) to maintain the systems and processes that are needed to ensure high-reliability operations. In addition, DOE needs to establish a safety research office(s), similar to NRC’s Office of Research, to help address immediate safety issues, as well as provide state-of-the-art research and testing capabilities to ensure the continuous improvement of complex activities such as facility design, safety analysis, and development of safety standards. This research would be in support of the needs of the proposed central safety authority.

#### **8.2.4 Technical Capability**

The slow degradation of technical expertise within DOE has been an ongoing issue raised by the Board in its letters, reports, and recommendations (Defense Nuclear Facilities Safety Board, 1993, 1996). Suggested improvements would be to:

- Require that senior line management positions with safety responsibilities have technical degrees in a relevant engineering or science discipline, plus demonstrated experience in nuclear safety.
- Establish minimum 5-year terms for those positions.
- Provide a training and qualification program run by recognized safety experts for these positions. This program would need to provide preparation and practice for managing off-normal and emergency events.
- Provide resources for the continual technical growth of safety professionals.

An additional approach to improving centralized technical expertise would be to empower the proposed NNSA and ESE nuclear safety officers to ensure the quality of safety professionals by authorizing them to review all hiring of technical staff in criticality safety, radiation protection, actinide materials, nuclear facility operations, risk analysis, and other key nuclear safety capabilities.

#### **8.2.5 Corrective Action Plans**

Many organizations within DOE have completed reviews and developed lessons learned from the Columbia accident. Corrective action plans from these reviews need to be integrated and acted upon. For example, NNSA has already taken action on some of the recommendations resulting from General Haeckel's review of the Columbia Accident Investigation Board Report. Other accidents and near-misses that have occurred in high-hazard industries form a basis for corrective actions that would improve the safety performance of DOE and its contractors. Currently, the Assistant Secretary for ES&H is responsible for measuring and tracking contractor performance and has several sources of information and dissemination systems.

No one in the DOE system is responsible for ensuring that DOE sites take corrective actions to learn from mistakes in other organizations. The responsibility for actually resolving safety issues is correctly being delegated to DOE's field offices, but headquarters needs to provide independent oversight to ensure that safety performance assessments are adequately tracking precursor incidents affecting nuclear safety and that lessons learned are being implemented across the complex. The central authority also has a role to develop and track corrective actions for cross-cutting issues that DOE has not resolved appropriately in the past because the responsibility for corrective actions has been uncoordinated and diffuse.

### **8.2.6 Integrated Safety Management**

Implementation of ISM is the key to improving safety attitude. DOE and its contractors have invested significant resources in defining, developing, and implementing ISM systems. However, good safety attitude must go beyond declarations. The real payoff will come from execution of the guiding principles and core functions of ISM at the organization, facility, and activity levels. In particular, senior leaders need to maintain a questioning attitude and insist and verify that ISM is being implemented at the activity level, where workers handle hazardous materials, operate nuclear facilities, and carry out hazardous activities. Especially for federal staff, increased formality in implementing ISM appears to be warranted. Greater attention needs to be focused on such issues as the capability and capacity to implement delegations of authority and expectations for implementing mechanisms to ensure that the principles of ISM are maintained as part of any organizational changes. A comprehensive ISM system verification review of DOE following implementation of the changes suggested in this report would be an important step.

### **8.3 Summary**

Complex system failures leading to high-consequence accidents are low-probability events whose roots lie in the interactions between engineering failures and human factors. The potential for these significant accidents is related to low-probability statistics, and organizations can be fooled by ignoring random events that occur too infrequently for the organization to benefit from traditional lessons-learned programs. Because the consequences are unacceptable, the weapons complex cannot afford a nuclear accident. While uncertainty cannot be eliminated, the likelihood of a nuclear accident can be reduced with rigorous nuclear safety organizational attributes.

The Board's Recommendation 2004-1 challenges some of the delegations and assigned roles in DOE's current organizational hierarchy. It is the Board's belief that the core nuclear safety governance functions that have been assigned or delegated to the Assistant Secretarial level or below should be reassigned to a central nuclear safety authority that is adequately staffed and funded to fulfill this function.

The recommended separation of responsibility and creation of a strong nuclear safety self-governance function should resolve many of the problems and negative trends that DOE has been experiencing. If the central safety authority maintains awareness of complex-wide nuclear safety issues, has the authority to order improvements, and has general control over nuclear safety research, the likelihood of a nuclear accident will be reduced. This organizational structure will promote a sustained "organizational shift" that should provide a better balance between the goals of productivity and safety.

## **APPENDIX: CHRONOLOGY OF KEY EVENTS IN DOE NUCLEAR SAFETY<sup>1</sup>**

A chronology of key events leading to the current state of DOE's ES&H program follows.

**1942–1946:** The development of nuclear weapons during World War II was performed in secrecy under the Manhattan Engineering District. The deadly effects of massive doses of radiation, as evidenced in the people of Hiroshima and Nagasaki, led to expanded research into radiation effects on people and the environment.

**1946–1960:** In 1946, Congress established the Atomic Energy Commission (AEC) to manage the nuclear weapons program. The AEC formed a Safety and Industrial Health Advisory Board to survey health, safety, and fire protection practices throughout the complex. In 1954, Congress changed the Atomic Energy Act to encompass peaceful uses of nuclear materials. Under the new Atomic Energy Act of 1954, Section 161, the AEC was authorized to “establish by rule, regulation, or order such standards and instructions to govern the possession and use of special nuclear material and by-product material as the Commission may deem necessary or desirable to promote the common defense, to protect or to minimize danger to life or property.”

In 1959, subject matter experts in applied health physics, fire protection, and industrial health and safety standards were consolidated into an Operational Safety Division. Independent AEC reviews and critiques of safety practices at weapon production facilities marked the first forceful federal insertion of nuclear safety expectations into the workplace. However, expert consensus—rather than demonstrated compliance with formalized safety requirements—was the basis for authorization. In effect, the 1946–1960 period was marked by a continuation of expert-based safety practices learned during the Manhattan Project, and subsequently augmented by the safety systems of the industrial firms with which the government contracted to run the weapons production facilities. The AEC relied upon its contractors to apply the results of the weapons laboratories' research on the biological effects of radiation on people and the environment, as well as of basic research in chemistry, physics, and metallurgy.

**1960–1980:** In 1961, the AEC's Director of Regulation was assigned authority to establish nuclear safety requirements. Commercial applications of nuclear energy were licensed through the formal rule-making process; however, the weapons establishment was not subject to formal licensing. New environmental protection statutes enacted during the 1970s forced major changes to the AEC's environmental program, and in 1973, the AEC created an Assistant General Manager for ES&H. The biology, medicine, and reactor research programs continued to provide basic safety-related data to support both the weapons program and the commercial regulatory program.

---

<sup>1</sup> This appendix is a synopsis of work done by Joseph DiNunno.

The Energy Reorganization Act of 1974 abolished the AEC and established the Energy Research and Development Administration (ERDA) and the independent NRC. ERDA and subsequently DOE assumed responsibility for the weapons program, including the legacy wastes of the early weapons production era; coordinated biomedical and environmental research; oversight of a health and safety laboratory; development of environmental control technologies; development of safety standards; compliance oversight; coordination of reactor safety research; and waste management and transportation.

**1980–1990:** The 1980s were marked by intensified public interest and involvement of activists in nuclear safety, triggered in part by the Three Mile Island reactor accident. Both the nation's weapons and commercial nuclear power programs were the focus of the activists' attention and growing concern about nuclear-related issues. Confidence in DOE's safety programs eroded, and residual radioactive wastes emerged as the major point of controversy. DOE's struggle with remedial actions was met with lawsuits and court actions, leading to the opening of DOE defense nuclear sites to access and scrutiny by the Environmental Protection Agency and state authorities. An Assistant Secretary position for ES&H with enhanced responsibilities and authority for safety in mission-oriented environmental cleanup and weapons program activities was created in 1985. In 1988, Congress established the Board to provide independent external oversight for defense nuclear facilities.<sup>2</sup> That same year, the Secretary of Energy undertook a major restructuring of DOE's approach to safety management. Line managers were made primarily responsible for safety management, oversight increased, and stringent technical safety standards for operating nuclear facilities were issued. The Price Anderson Amendments Act of 1988 authorized DOE to impose civil penalties on indemnified contractors to ensure compliance with nuclear safety requirements. DOE's Office of Price Anderson Enforcement was subsequently formed to investigate potential violations of enforceable requirements and initiate enforcement actions.

**1990–2000:** During the 1990s, DOE's ES&H program continued to experience shifts in direction as both Congress and the Administration worked to solve the problems of nuclear waste and surplus nuclear materials resulting from the shutdown of weapons production lines. In 1992, Congress passed the Federal Facility Compliance Act, requiring federal agencies to bring their facilities into compliance with federal environmental protection requirements.

During the mid-1990s, DOE orders and manuals were reduced to contain only high-level safety expectations, which are generally applicable to most of DOE's defense nuclear work. More explicit "how-to" or process-related direction was extracted and placed in guides and standards. The structure of DOE's directives system implied that most of the safety expectations set forth in orders and manuals should be included as safety requirements in contracts. As before, none of the direction from DOE (other than requirements in rules) is binding on contractors unless it is included in their contract. The intent under this system is for DOE's contractors and the contracting officers to use a standards and requirements identification process to select a set of binding safety requirements that is graded to the work at contract sites. Those safety

---

<sup>2</sup>The Board began operations in October 1989.

expectations, regardless of their original source, then become contractually binding safety requirements. This list is referred to as “List B” in Section 970.5204-2 of the Department of Energy Acquisition Regulations. List B is used in conjunction with 10 CFR Part 830 to form the nuclear safety requirements for the contractor.

## REFERENCES

- American Nuclear Society. 2000. *Reactor Safety*, Position Statement.
- Cantelon and Williams, R. C. 1982. *Crisis Contained: The Department of Energy at Three Mile Island*.
- Chiles, J. R. 2001. *Inviting Disaster*.
- Code of Federal Regulations. 2004a. 10 CFR Part 820. *Procedural Rules for DOE Nuclear Activities*.
- Code of Federal Regulations. 2004b. 10 CFR Part 830, *Nuclear Safety Management*.
- Columbia Accident Investigation Board. 2003. *Columbia Accident Investigation Board Report*.
- Defense Nuclear Facilities Safety Board. 1996. *An Assessment Concerning Safety at Defense Nuclear Facilities: The DOE Technical Personnel Problem*. Technical Report DNFSB/TECH-10. Washington, DC.
- Defense Nuclear Facilities Safety Board. 1993. *Recommendation 93-3: Improving DOE Technical Capability*. Washington, DC.
- Institute of Nuclear Power Operations. 1999. *Principles for Effective Self-Assessment and Corrective Action Programs*.
- Krause, T. R. 1995. *Employee-Driven Systems for Safe Behavior*.
- LaPorte, T. R. 1996. "High Reliability Organizations: Unlikely, Demanding and At Risk," Journal of Contingencies and Crisis Management, Vol. 4, No. 2, June.
- Los Alamos National Laboratory. 2000. *A Review of Criticality Accidents*. LA-13638.
- Matthews, B. 1998. "Institutional Constancy Guides NMT's Future," The Actinide Research Quarterly. 1<sup>st</sup> quarter.
- Medvedev, G. 1991. *The Truth about Chernobyl*.
- National Aeronautics and Space Administration and Naval Sea Systems Command. 2002. *NASA/Navy Benchmarking Exchange (NNBE)*, Volume 1.



National Nuclear Security Administration. 2004. *NNSA Lessons Learned and Recommendations from Review of NASA's Columbia Accident Investigation Board Report*.

Perrow, C. 1999. *Normal Accidents: Living with high Risk Technologies*.

Reason, J. 1997. *Managing the Risks of Organizational Accidents*.

Roberts, K. H. 1990. "Some Characteristics of One Type of High Reliability Organization." *Organizational Science*, Vol. 1, No. 2.

Rochiln, G. I. 1996. "Reliable Organizations: Present Research and Future Directions," Journal of Contingencies and Crises Management, Vol. 4, No. 2.

Sagan, S. D. 1993. *The Limits of Safety*.

Snook, S. A. 2000, *Friendly Fire*.

Travers, W. D. Executive Director for Operations, Nuclear Regulatory Commission. 2002. Memo to A. T. Howell, III, Director, Division of Reactor Safety Region IV, Concerning Davis-Besse Reactor Vessel Head Degradation—Lessons-Learned Task Force and Charter.

U.S. General Accounting Office. 2004. *NRC Needs to More Aggressively and Comprehensively Resolve Issues Related to the Davis-Besse Nuclear Power Plant's Shutdown*, GAO-04-415.

Public Law 93-438, 99 Stat. 1233, Energy Reorganization Act of 1974.

U.S. Department of Energy. 1996. DOE P 450.4, *Safety Management System Policy*.

Public Law 100-406, 102 Stat. 1066. *Price Anderson Amendments Act of 1988*.

U.S. Department of Energy. 2004. *The Department's Reporting of Occupational Injuries and Illnesses*. Office of Inspector General, Office of Audit Services. DOE/IG-0648.

U.S. Department of Energy. 2003. *Competing the Management Operations Contracts for DOE's National Laboratories*.

Vaughan, D. 1996. *The Challenger Launch Decision*.

Weick, Karl. 1987. "Organizational Culture as a Source of High Reliability."

## **GLOSSARY OF ACRONYMS AND TERMS**

<b>Abbreviation</b>	<b>Definition</b>
AEC	Atomic Energy Commission
Board	Defense Nuclear Facilities Safety Board
CFR	Code of Federal Regulations
DOE	Department of Energy
ERDA	Energy Research and Development Administration
ESE	Office of Energy, Science, and Environment
ES&H	Office of Environment, Safety, and Health
LWC	Lost Workday Case
NASA	National Aeronautics and Space Administration
NNSA	National Nuclear Security Administration
NRC	Nuclear Regulatory Commission
SUBSAFE	Submarine Safety
TRC	Total Recordable Case